**Česká zemědělská univerzita v Praze**

**Provozně ekonomická fakulta**

**Katedra informačních technologií**


# Diplomová práce

# Bezpečnost systémů multifunkčních karet

**Radomír Kozler**

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Bezpečnost systémů multifunkčních karet" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Plzni dne 3.4.2011 _____

Poděkování

Rád bych touto cestou poděkoval vedoucí diplomové práce RNDr. Dagmar Brechlerové, Ph.D. za odborné rady a pomoc, dále Mgr. Martinu Chvalovi a Zbyňku Proškovi, členům týmu Plzeňské karty za pomoc při získávání informací.

# Bezpečnost systémů multifunkčních karet

---

# Security of multifunctional card systém

Souhrn

Cílem této diplomové práce je stanovit rozdíly mezi běžným podnikovým nebo jiným IT systémem a IT systémem multifunkčních karet. Na základě zjištěných rozdílů pak vypracovat základní bezpečnostní dokumentaci systému multifunkční karty a to v rozsahu tří základních dokumentů. Dokumenty „Bezpečnostní politika“, „Bezpečnostní řád“ a „Analýza rizik“.
Základem pro práci tak je analýza rozdílů mezi takovými dvěma systémy v běžně užívané konfiguraci. Po vyhodnocení relevantních rozdílů pak je na základě „best of practices“ z běžných informačních systémů aplikovaných na systém multifunkční čipové karty vytvořena bezpečnostní dokumentace, která je využitelná jako možný vzor pro tvorbu konkrétní bezpečnostní dokumentace.

Summary

The aim is to determine the differences between a standard or other enterprise information system and information system multifunction cards. Basic safety documentation will be prepared on the basis of the differences found for the multifunction card system. Documentation will include three papers, „Security Policy“, „Safety Regulations“ and Risk analysis. It is based on work analysis of the differences between the two systems commonly used configuration. Security documentation is created after the evaluation of relevant differences. It is based on „best of practices“ of current information systems. The rules are applied to a system of multifunctional smart cards. Security documentation is usable as a possible model for the creation of a specific security documentation.

**Klíčová slova:** čipová karta, bezpečnost, Mifare, DESFire, elektronická peněženka, multifunkční karta.

**Keywords**: chip card, security, Mifare, DESFire, electronic wallet, multitifunctional card,.

# Obsah

# 1. Úvod

Veřejný internet, firemní sítě, osobní počítače jsou vystaveny nepřetržitému nebezpečí útoků počítačových pirátů, hackerů, vlastních zvídavých uživatelů a to za pomoci nebo prostřednictvím různých malware, spyware, virů, trojských koní a dalších a dalších hrozeb. Taková je cena za možnosti, které moderní IT svět poskytuje a s těmito hrozbami se snaží vypořádat jak běžní uživatelé, tak specialisté v počítačové bezpečnosti, a to za pomoci nebo prostřednictvím opět mnoha různých nástrojů. Na druhé straně barikády tak stojí firewall, antivir, VPN, a ve firemních systémech především metodiky, které určují, jak se mají jednotliví uživatelé chovat, jaké bezpečnostní nástroje mají být v systému použity, jak často se má kontrolovat, dohlížet.

Tvorba bezpečnostní metodiky se pak děje zevnitř vlastními lidmi, čistě dodavatelsky, případně kombinací obou těchto způsobů. Velmi zajímavý názor byl zveřejněn na serveru Lupa.cz v článku IT bezpečnost je předražená.

„Agentura Gartner, která platí za jednu z největších autorit, pokud jde o výzkum a analýzu trhů v oblasti IT, ústy svého viceprezidenta pro výzkum přišla nedávno s velmi zajímavou myšlenkou. Touto myšlenkou je, že zejména velké podniky platí za používání bezpečnostních produktů podstatně více, než by měly, a že je tyto produkty často chrání méně, než se domnívají. Terčem jeho kritiky se stali zejména dodavatelé firewallů a antivirového softwaru, kteří prý (Gartner má na to data a celé prohlášení bylo výstupem poměrně dlouhého výzkumu) zachovávají zastaralé obchodní modely s vysokým ziskem při nízkém, či dokonce klesajícím benefitu pro zákazníka. Jinými slovy, Gartner se domnívá, že zákazníci (mají tím na mysli větší firmy, ale není problém převést tento stav i na menší) jsou svými bezpečnostními dodavateli vydíráni – a měli by s tím něco dělat. (1)“

Dále se v článku uvádí, že reálná úroveň bezpečnosti uživatelů klesá – nehledě na skutečnost, že žádná kombinace bezpečnostních řešení technicky není schopna vzdorovat všem myslitelným rizikům. Klasické komerční firmy působící převážně v ČR, které mají přes 200 zaměstnanců, investují do výpočetní techniky řádově desítky milionů korun ročně. Z toho podíl na bezpečnosti činí obvykle okolo 30 procent. (2) Z vlastní zkušenosti mohu ve shodě s uvedenými názory potvrdit, že většina odborných správců, implementátorů a analytiků informačních systémů si předchozí tezi, zde ovšem zcela explicitně argumentovanou, uvědomuje, či ji má přinejmenším v povědomí. Informační systémy v síťovém prostředí nejsou absolutně bezpečné, k tomuto stavu se lze současnými technickými možnostmi pouze přiblížit, a obchodní, technické ani licenční strategie dodavatelů jednotlivých komponent

tomu příliš nenapomáhají. Na druhé straně dodavatelé bezpečnostních řešení v metodické oblasti přichází s výbornými zkušenostmi, které však poněkud mechanicky aplikují na ošetřovaný systém. Můžeme například  Tato nepříliš vhodná praxe způsobuje to, že dokumentace vytvořená těmito firmami výborně vypadá, ve skutečnosti ji však mnohdy nelze plnit. Velkým nešvarem je pak přenesení mnoha odpovědností a povinností na různé úrovně řídící struktury u zadavatele. To by bylo samozřejmě v pořádku, pokud by na to byl zadavatel v předávacím protokolu upozorněn. Skutečnost je však taková, že dodaná výborně vypadající bezpečnostní dokumentace se hemží termíny, jako je například:

Systémy musí zajistit častou změnu hesel, archivace logů se řídí skartačním řádem společnosti, obrazovka monitoru nesmí být natočena tak, aby na ni klient viděl, incidenty jsou pravidelně zaznamenávány do deníku incidentů.

Nikdo však zadavatele neupozorní a někdy se ho ani nezeptá, zda nějaký deník incidentů nebo skartační řád existuje, vůbec už pak, jestli pamatuje na zmíněnou archivaci logů, či zda jsou uživatelé seznámeni s tím, že mají incidenty hlásit, a zda vůbec vědí, co je za incident považováno. Dochází tak k paradoxním situacím, kdy podnik má i implementován drahý systém na evidenci incidentů, pokud však v rámci penetračního testu k němu dorazí zcela neznámý člověk a prohlásí, že si jde pro jeho tiskárnu, která vykazuje chybu, bez základní úvahy, že žádnou vadu nehlásil, tiskárnu odevzdá a neznámý s ní hrdě odkráčí středem fronty. Až po týdnu začne nespokojený uživatel IT oddělení bombardovat dotazy, kdy mu „prachdudynecky“ už tu tiskárnu vrátí.

Po takovém zjištění následuje červenající se zápis z penetračních testů, se kterým se seznámí pouze nejužší vedení společnosti a to z toho důvodu, že takový zápis je „velký tajem“ (výraz jsem si půjčil ze hry Hrdý budžes“). Myslíte, že následuje briskní náprava? Výsledek úvahy nechám na Vás.

Celý uvedený příklad byl z implementací bezpečnosti na běžný informační systém.

Konzultant vždy úspěšně dokončil práci, předal sofistikovanou bezpečnostní dokumentaci, nicméně jejím fungováním v praxi se až do penetračních testů nikdo nezabýval. Je dlužno přiznat i to, že podobné nedokonalosti odhalí na informační bezpečnost specializovaný audit, zůstává ale otázkou, kolik firem si ho ještě objedná poté, co zaplatily stovky tisíc za bezpečnostní dokumentaci a zabezpečení, které jim doporučili zmínění dodavatelé bezpečnostních řešení. Pro tento okamžik se spokojím s tvrzením, že přístup k tvorbě bezpečnostní dokumentace je u projektů multifunkčních karet stejný, nebo velmi podobný. Střet s realitou pak někdy nezpůsobí penetrační testy, ale daleko hůře opravdový útok zvenčí.

Pokud je takový útok patřičným způsobem medializován, způsobí problémy celému projektu na mnoho let.

## 2. Cíl práce a metodika

Cílem práce je na základě určení identifikace rozdílů mezi běžným IT systémem a systémem multifunkční karty vytvořit tři základní bezpečnostní dokumenty pro systém multifunkční čipové karty. Jedná se o „Analýzu rizik“ „Bezpečnostní politiku“ a „Bezpečnostní řád“. Jako vzorek běžného IT systému bude brán systém běžné akciové společnosti s obratem několika set milionů korun, existujícím IT oddělením, několika detašovanými pracovišti a implementovaným podnikovým informačním systémem.

Jako vzorek systému multifunkční karty bude brán systém městské multifunkční karty, který umožňuje držiteli takové karty zjednodušeným způsobem čerpat služby a to placené ze strany držitele, tak i hrazené například městem, zpravidla v urbanizovaném prostředí. Jako atribut přiřadíme ještě využívání elektronických peněz na takovéto kartě. Pro bližší představu si ji určeme jako ekvivalent pražské Open card, Plzeňské karty, Liberecké Opus card, či IN karty Českých drah.

Jako metoda pak je užito běžných analytických postupů při tvorbě bezpečnostní dokumentace, spolu s přihlédnutím ke zjištěným atributům informačního systému multifunkční karty a k různým normovaným systémům řešícím problematiku počítačové bezpečnosti, k vytvoření možné základní bezpečnostní dokumentace systému multifunkční karty, která respektuje zjištěné rozdíly a upravuje případně použité „best of practices“ tak, aby je bylo v takovém systému možné reálně dodržovat. Vzhledem ke skutečnosti, že řešení je tvořeno nad virtuálním problémem, nepřiřadíme mu ani jeden z normovaných bezpečnostních systémů, ale pokusíme se ho vytvořit tak, aby byl pod těmito systémy aplikovatelný, laicky řečeno aby pod ně šla dokumentace „ohnout“. Doporučení, jak řešit nejzávažnější zjištěné rozdíly (pokud jsou řešitelné) pak je uvedeno v závěru práce

# 3. Literární rešerše

## 3.1. Úvod do problematiky

### 3.1.1. Řešení bezpečnosti v IT systémech

Bezpečnost v IT systémech se dostává v posledních letech do popředí zájmu, a to jak laické veřejnosti, tak managementu subjektů, které takové systémy spravují nebo vlastní. Správa informační bezpečnosti je nutná pro bezproblémový chod organizace. Historicky první uznanou normou o počítačové bezpečnosti bylo uznání **Kritéria hodnocení důvěryhodných výpočetních systémů** normou Ministerstva obrany USA. Série vzniklá na tomto základě dnes již čítá desítky publikací. (3) „Přesto z průzkumů v roce 2003 vyplývá, že až 54% organizací v ČR nemá formálně definovanou a nejvyšším vedením přijatou bezpečnostní politiku. (4) Pro běžné podnikové systémy IT existují ověřené metody tzv. „best of practices“ které umožňují takové systémy bezpečnostně patřičně ošetřit. Tato práce se věnuje metodologii bezpečnosti, tedy tomu, jak pomocí správně vytvořené bezpečnostní dokumentace zajistit bezpečnost vlastní, tedy fyzickou. V okamžiku, kdy se pokusíme takové „best of practices“ aplikovat na systém multifunkční čipové karty, zjišťujeme, že část pravidel je v praxi nepoužitelná vůbec, případně při pokusu o jejich dodržování narážíme na organizační, právní a i technické problémy, které u běžného IT systému neexistují. Pro práci se budu snažit použít **systémový přístup,** za který je považovaný způsob myšlení, způsob řešení problému či způsob jednání, při němž jsou jevy chápány komplexně ve všech vnějších i vnitřních souvislostech. (5) Systémový přístup také znamená naplnit jednotlivé etapy životního cyklu řešením bezpečnosti, jako jsou:bezpečnostní politika, analýza rizik, zvládání rizik v souladu s bezpečnostním projektem, implementace a testování, bezpečnostní dokumentace, provoz, monitorování účinnosti implementovaných bezpečnostních opatření, změnové řízení. (6) ČSN, zvláště harmonizované normy jsou cenným zdrojem informací a inspirace pro tvorbu jakéhokoli druhu bezpečnosti. Velmi důležitou myšlenku můžeme najít i v definici bezpečnostní strategie od Garfinkela. Všichni zaměstnanci se podílejí na zodpovědnosti za ochranu a dohled nad informacemi, které se vytvářejí, zpracovávají, přijímají nebo odesílají v jejich oddělení. (7) Pocit odpovědnosti každého jednotlivce a jeho následné zakotvení v bezpečnostní dokumentaci je třeba považovat za základní stavební kámen dobré bezpečnostní dokumentace. Personální

bezpečnosti ale nespočívá jen v dohledu nad informacemi. Většina systémů je ohrožena právě lidmi uvnitř systému, vlastními zaměstnanci organizace. Vedení, management organizace by měl předpokládat, že může zaměstnávat lidi, kteří svými morálními vlastnostmi neodpovídají požadavkům na ně kladeným. (8) I s tímto faktem je nutno pracovat a toto riziko řídit. Mnou pociťovaný problém s nekritickým přenášením zavedených schémat identifikoval ve své knize i Josef Požár. Pokud má jedna společnost kvalitní politiku, (myšleno bezpečnostní), tak není zaručeno, že její přenesení do druhé společnosti bude stejně kvalitní. Vylepšování „vzoru" bez předchozí analýzy tedy může přinést velice špatný výsledek. (9) V práci se budu zabývat i členěním dat z pohledu jejich důvěrnosti. Data lze dělit například na veřejná, citlivá, důvěrná a tajná. (10) Způsobů dělení je samozřejmě mnoho, zabývá se jím i Zákon č.101/200 Sb.o ochraně osobních údajů. Tam lze zjistit, která data jsou „citlivá" z pohledu zákona.

## 3.2. Podnikový IT systém

### 3.2.1. Softwarová řešení

Podnikový IT systém včetně jeho software i hardware slouží především k lepším možnostem řízení podniku. Snahou je vytvořit v řešení IS/IT takovou skladbu softwarových a technických prostředků a doprovodných služeb, které budou nejlépe odpovídat situaci a potřebám podniku (z hlediska kvality, výkonových a kapacitních parametrů atd.) dále se podnik snaží dosáhnout optimálního poměru cena / výkon z hlediska celého IS/IT, tj. potřebného výkonu za přiměřenou cenu. Vzhledem k dnešní jisté uniformitě pak v takové běžné akciové společnosti s obratem několika set milionů korun nalézáme zpravidla následující softwarová řešení, plnící každý svůj specifický účel.

CRM systém

CRM je zkratka z anglického Customer Relationship Management a slouží k označení systémů pro řízení vztahů se zákazníky. Jedná se o programy, které umožňují shromažďovat, třídit a zpracovávat údaje o zákaznících, vytvářet databázi jejich kontaktů, probíhající obchodní procesy a dosahované tržby. Dále jsou využívány pro ukládání informací o jemných specifikách jednotlivých obchodních partnerů a vztazích s nimi, tak aby byly využitelné v dalších obchodních případech. CRM systémy tak pomáhají sledovat a vyhodnocovat veškeré obchodní aktivity v rámci celé společnosti. Jako vhodný doplněk bývají součástí CRM systémů nejrůznější statistické moduly. Cílem CRM systémů je zlepšit cílení služeb, výrazněji porozumět zákazníkům a rozdílům mezi nimi a identifikovat jejich konkrétní

potřeby. To jako celek při správném využití má umožnit budovat dlouhodobě prosperující vztahy se zákazníky a tím maximalizovat zisk z jednoho zákazníka. Protože stávající zákazníci jsou pro firmu nejlepší (úsloví „ lepší vrabec v hrsti než holub na střeše“, případně „není problém zákazníka získat, ale udržet si ho“), vyplatí se za podpory CRM systémů zajistit si jejich věrnost a důkladně o ně pečovat.

ERP systémy

Zkratkou ERP (Enterprise Resource Planning) jsou v dnešní době označovány komplexní informační systémy organizací, integrující činnosti související s financemi, účetnictvím, CRM, řízení lidských zdrojů, výrobou, dodavateli, skladovým hospodářstvím atd. Oproti dřívějšímu trendu, kdy jednotlivou oblast firma řešila samostatnými dílčími softwary, dnes se prosazuje trend volby jednoho zastřešujícího ERP systému, který pokrývá veškeré potřeby organizace. ERP systémy integrují veškerá data a procesy organizace do unifikovaného celku. Typický ERP systém dosahuje integrace těchto dat za pomoci množství softwarových komponent (modulů) a náročné hardwarové infrastruktury. Základní a nosnou ingrediencí typických ERP systémů je použití jedné databáze k ukládání dat. Tuto centrální databázi pak využívají všechny moduly v systému nainstalované. ERP systémy se tak pokoušejí pokrýt všechny základní funkce podniku, nehledě na typ organizace nebo její činnosti. Stejný systém tak dnes používají akciové společnosti, municipality, státní instituce a další velké organizační složky založené za nejrůznějšími účely. Tato univerzalita je však dle mého názoru i největším nedostatkem ERP systémů. Jejich customizace je velmi nákladná a mnohdy do detailu prakticky nemožná. Proto jsou dále popsány i jednotlivé typické SW aplikace, jak jsou dnes jednotlivými podniky z výše uvedeného důvodu mnohdy využívány i vedle masivního ERP systému.

Účetní SW

Základním cílem účetnictví je podávat pravdivý a věrný obraz o finanční, výnosové situací a majetku podniku.

K tomuto cíli směřuje i základní obsah této programové výbavy. Jedná se o moduly určené k fakturaci, vedení pohledávek, mzdové moduly, moduly řešící vnitropodnikové účetnictví.

Skladový SW

U větších společností se velmi často setkáváme i se specializovaným skladovým software. Jistou zajímavostí je, že se mnohdy jedná o do té míry customizovanými aplikacemi, že už se jedná o samostatné větve původního programátorského záměru. Tento SW slouží k evidenci

materiálu, příjmu na sklad, výdeji ze skladu, evidenci materiálu v pobočných skladech, hlídání minimálních a maximálních zásob u jednotlivých druhů materiálu nebo zboží.

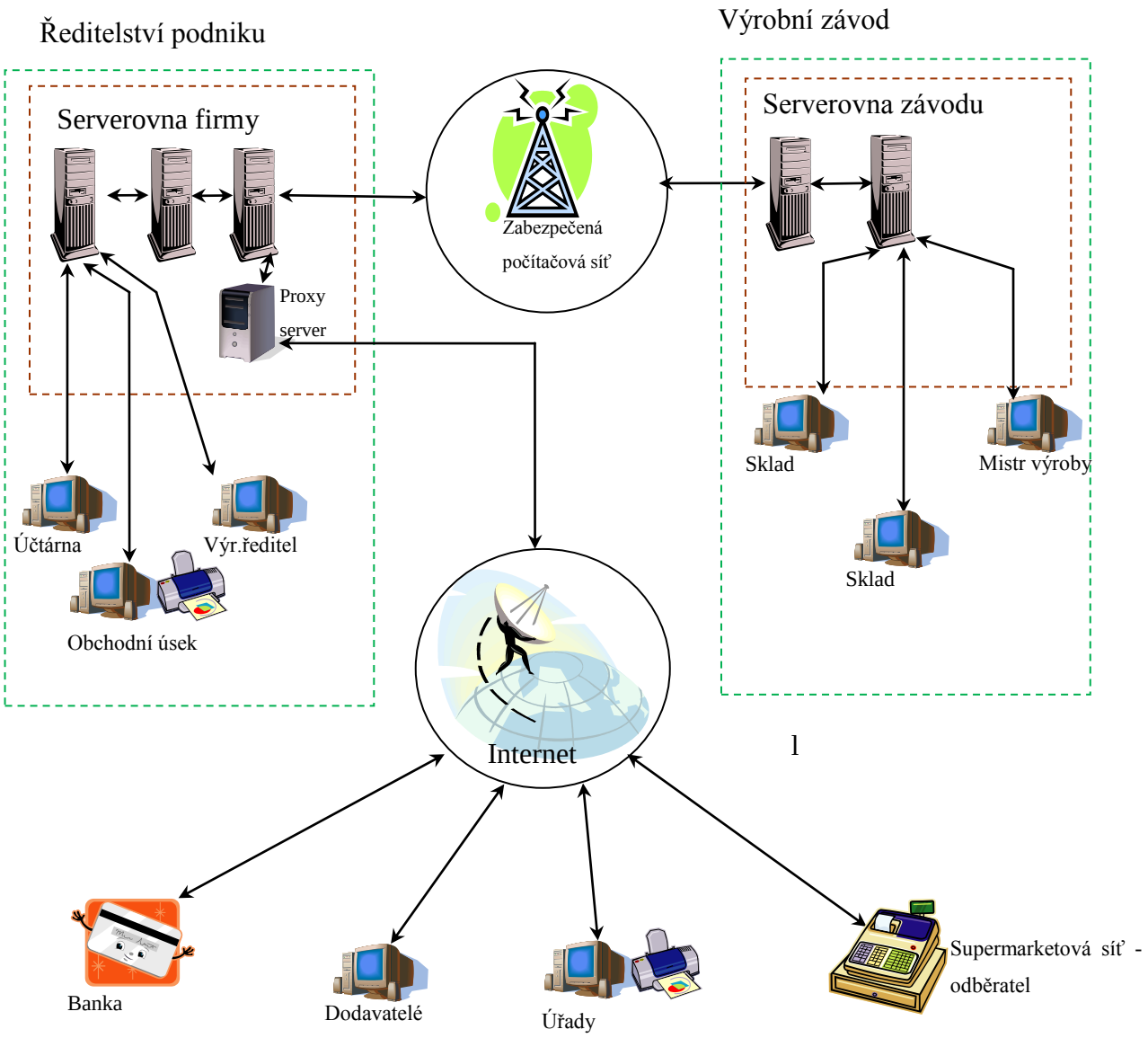
Ostatní SW

Dále lze u velkých firem samozřejmě nalézt řadu dalších aplikací. Takové aplikace však zpravidla již úzce souvisí s hlavním předmětem podnikání firmy a proto je nalézáme jen v některých organizacích. Může se jednat o vyšší programovací nástroje u SW firem, nástroje pro architekturu, projektování technologických i stavebních celků, medicínské aplikace, aplikace pro řízení dopravy atd.

### 3.2.2. Řešení infrastruktury

V takto definovaném typickém podniku nalézáme zpravidla, stejně jako u SW, řešení infrastruktury, které je do jisté míry uniformní. Uniformita zde není myšlena nijak hanlivě, naopak ji chápeme jako řešení vycházející z „ best of solutions“ a pro firmu je jednoznačně přínosné. O struktuře popsané v následujícím schématu lze samozřejmě vést diskuse, v současné době se jako velmi módní řešení využívají datová úložiště mimo serverovny firmy, případně se poskytování serverové kapacity děje outsourcingem jako celek. Na základě znalosti prostředí však uvažujme jako pro dnešní dobu typickou následující strukturu. Je třeba dodat, že na následně popsanou strukturu je zpravidla aplikována i bezpečnostní dokumentace. Obrázek slouží pouze jako schéma, nad kterým jsou vedeny další úvahy, nejsou v něm zakresleny běžné bezpečnostní prvky. Pokud řešíme bezpečnost od začátku, musíme vzít v úvahu i to, že aplikujeme bezpečnostní opatření nad infrastrukturou, kterou v úvahách od již aplikovaných opatření očistíme. To nám umožňuje uplatnit „helicopter view“, kdy můžeme řešit věci i jinak, lépe a levněji než je nasměroval někdo před námi.

obr. číslo 1 – Schéma běžného informačního systému




### 3.3. Systém multifunkční karty

Zde je uveden popis systémů multifunkčních karet - využito z BP Kozler (11)

Systémy mutifunkčních čipových karet využívají dvou základních principů. Jedním je využití jedinečného ID karty, které je spřaženo v systému s osobními daty držitele karty. Na vlastní

čipové kartě pak neleží žádná aplikace a všechna data jsou držena a zpracovávána v systému využívajícím toto ID. Používá se pro něj označení „identifikační funkce karty“.
Druhý princip je sofistikovanější a využívá datový prostor na kartě k uložení různých informací. Typickým příkladem takového využití je elektronická peněženka. Dochází k rozsáhlé komunikaci s vnitřním čipem karty, čtení, zápisu a to s sebou přináší rozsáhlejší možnosti využití, ale současně i větší nároky na obslužný software i samotné čtečky těchto karet. Takový systém typicky zahrnuje využití karty pro veřejnou dopravu, docházkové a přístupové systémy, pro platby za parkování, jako knihovní průkaz, identifikaci ve školních jídelnách pro odběr stravy a mnoho dalších.

## 3.1. Popis základního systému multifunkční čipové karty

Aby systém multifunkční čipové karty mohl začít fungovat, musí být vytvořen systém, který je schopen kartu vyrobit (naprogramovat, napersonifikovat). Tím je takzvané Kartové centrum. Úkolem tohoto centra je vedle vlastní výroby karet také uchovávat informace o jednotlivých držitelích karty, archivovat žádosti o karty, zhotovovat duplikáty karet v případě ztráty nebo nefunkčnosti, vytvářet seznam zakázaných karet (BlackList) apod.

### 3.1.1. Popis Kartového centra

Základem Kartového centra je databázový systém, v němž jsou všichni držitelé karet registrováni společně s informacemi o veškerých vydaných kartách, které byly v systému vytvořeny. Nad daty centra funguje aplikace, která zajistí potisk karet na speciálních tiskárnách. Zároveň tato aplikace zajistí naformátování potřebných paměťových oblastí v čipu karty a nastavení elektronických bezpečnostních prvků. Systém Kartového centra dále vytváří účetní a statistické sestavy, které slouží ke kontrolním nebo optimalizačním procesům.

### 3.1.2. Odbavovací systém Kartového centra

Odbavovací systém může být buď samostatná aplikace, nebo součást Kartového centra. Úkolem Kartového centra je provádět základní operace, jaké bývají po kartě vyžadovány – nahrávání časových jízdenek sloužících pro dopravu, nabíjení elektronické peněženky na kartě, případně práce s dalšími aplikacemi, jsou-li na Kartě uloženy. Vzhledem k tomu, že odbavovací systém využívá databází Kartového centra, využívá se spojení obou systémů do

jednoho. Výhoda tohoto řešení je i v tom, že je spravována pouze jedna aplikace pro výrobu i práci s kartami. Jako nevýhoda může být vnímáno praktické spojení dvou databází tvořených s nepatrně odlišným účelem do jedné. Z pohledu zákona se však jedná o databázi jedinou a proto je řešení legislativně možné.

### 3.1.3. Vybavení modelového Kartového centra  multifunkční karty

Kartové centrum může být tvořeno několika základními prvky:

- datová a systémová základna
- personifikační pracoviště
- archiv žádostí

Datová a systémová základna je společná pro celý systém multifunkční čipové karty, proto musí být dimenzována na předpokládanou kapacitu klientů. Zde je uloženo vlastní programové jádro celého karetního systému a datové úložiště pro uchování dat o klientech systému a kartách, které jsou těmto klientům přiřazeny. Vybavení této modelové základny může být například takovéto:

- aplikační server
- HW – výkonný server
- operační systém
- aplikační SW
- primární databázový server
- HW – výkonný server s kvalitním zálohovacím zařízením
- operační systém
- databázový systém
- zálohovací systém
- sekundární databázový server
- HW – výkonný server s kvalitním zálohovacím zařízením
- operační systém
- databázový systém
- zálohovací systém

Duplicita databázových serverů, které jsou propojeny replikačním systémem zajišťujícím synchronizaci databází na obou serverech v reálném čase, je doporučována z důvodu vysokého důrazu na zabezpečení dat v systému, jak je uvedeno v literatuře. (12)

Personifikační pracoviště je místo, kde probíhá vlastní výroba karet podle požadavků zákazníků na žádosti o výrobu karty. Toto pracoviště může být buď řešeno jednoúčelově – budou se zde karty pouze vyrábět, nebo může být kombinováno s odbavovací přepážkou, což umožní nabízet speciální služby – např. výroba karty na počkání apod. Kombinované řešení navíc využívá pracovní síly obsluhy pracoviště efektivněji.
Vybavení personifikačního pracoviště :

- PC (+ operační a antivirový systém)
- licence programu odbavovacího systému
- tiskárna daňových dokladů
- čtečka čipových karet
- UPS
- pokladní zásuvka pro uschování operativní hotovosti
- tiskárna pro potisk BČK
- scanner pro snímání fotografií ze žádosti

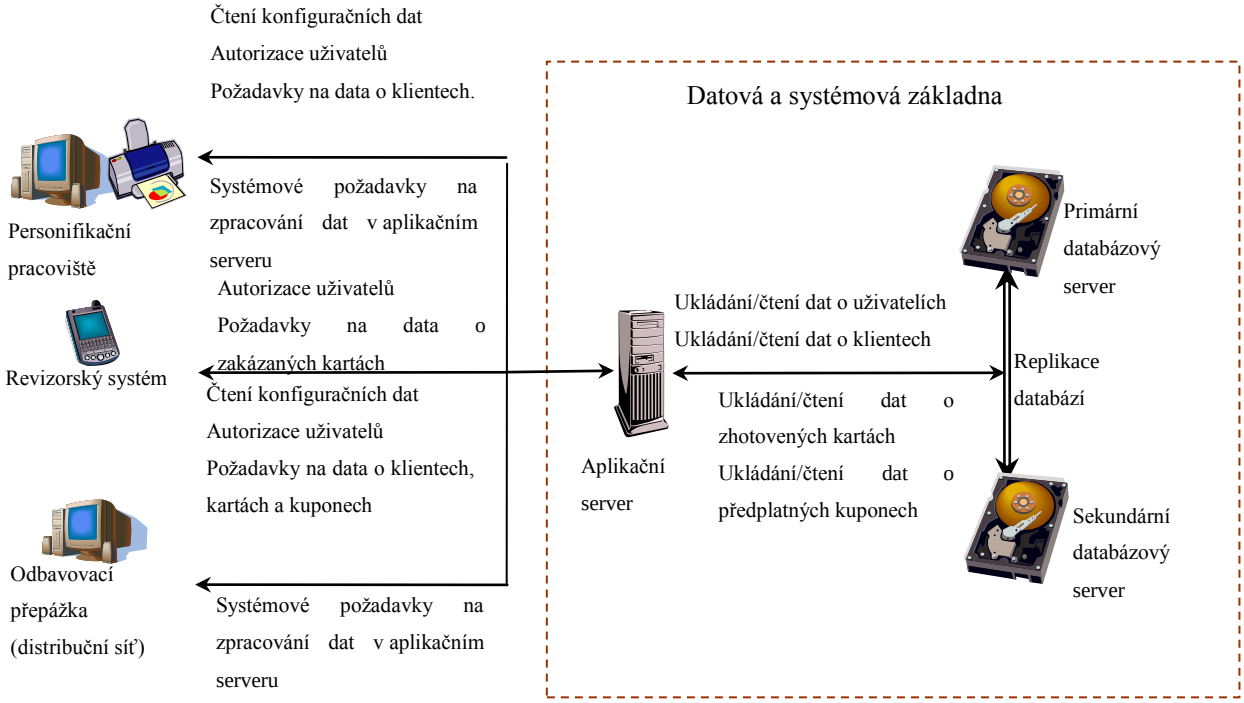
V místě personifikačních pracovišť pak je předpokládáno sdílené vybavení:

- tiskárna pro tisk pokladních uzávěrek
- kopírka

Kartové centrum může obsahovat buď jedno masivní personifikační pracoviště, které je řešit veškerou výrobu karet pro systém městské čipové karty, nebo může být zbudována síť personifikačních pracovišť tak, aby např. každá větší čtvrť měla jedno personifikační pracoviště (a tedy místo, kde je možno karty vyrábět na počkání).

Revizorský systém je zmíněn z toho důvodu, že základem pro systémy městských čipových karet je dopravní aplikace pro použití v MHD. Tento systém je tak nutnou nadstavbou a slouží jako support pro odbavení cestujících v MHD.

Obrázek 2 Modelové schéma řešení Kartového centra a odbavovacího systému městské čipové karty (11)




### 3.1.4. Zúčtovací centrum městské čipové karty

Jednou z nejdůležitějších aplikací v systémech multifunkčních čipových karet je elektronická peněženka. Zúčtovací centrum je databázový systém, který shromažďuje data o použití elektronické peněženky u jednotlivých partnerů, provádí potřebné kontrolní algoritmy a v dohodnutých termínech vyhodnocuje stav vzájemných pohledávek mezi jednotlivými subjekty zúčtování. Velmi důležité je si uvědomit, že standardním řešením pro provoz

zúčtovacího centra je jeho outsourcing. V současné době existuje v České republice pouze jedno dostatečně masivní zúčtovací centrum a to zúčtovací centrum ČSAD SVT. Další masivně využívané zúčtovací centrum je firmy EM TEST na Slovensku. Do tohoto centra se data o provedených transakcích z Čech zasílají ke zpracování a po jejich zpracování se opět importují zpět do systémů jednotlivých vydavatelů karet. Dlužno dodat (i když informací z této oblasti vzhledem k utajení je velmi málo), že slovenské řešení se chová jako typický black box, u českého centra je dodavatel otevřenější a vydavatelům karet je algoritmy zúčtování ochoten více otevřít. Pro vyrovnání vzájemných pohledávek připravuje zúčtovací centrum potřebné doklady. V systému multifunkční čipové karty se zpravidla vyskytuje více subjektů s různými odbavovacími a pokladními systémy a je nutno zajistit jednotný způsob předávání dat včetně definice struktury datových souborů. Předávání dat musí být zabezpečené proti neoprávněnému odečtení nebo modifikaci zasílaných souborů s jednoznačným kontrolním mechanismem informujícím zúčastněné subjekty o úspěšnosti přenosu a zpracování datových souborů, jak je uvedeno v literatuře (12) .

### 3.1.5. Přístup k datům v Zúčtovacím centru městské čipové karty

Každý subjekt zúčastněný v systému akceptace elektronických peněz systému městské čipové karty musí mít možnost nahlížet do dat uložených v zúčtovacím centru, pokud byla tato data pořízena na jeho provozovnách. Důvodem je možnost kontroly správnosti zúčtovacích procesů. Vydavatel elektronických peněz na městské čipové kartě musí mít absolutní přehled o všech transakcích, které jsou s jeho elektronickými penězi prováděny, a to proto, aby byl schopen řešit reklamace při práci s elektronickou peněženkou. Proto musí zúčtovací centrum umožňovat i kompletní přístup k datům na úrovni čtení.

### 3.1.6. Kontrolní mechanismy Zúčtovacího centra multifunkční čipové karty

Zúčtovací centrum musí provádět kontrolní procedury, které budou hlídat bezpečnost celého systému. Mezi kontrolní procedury patří např.:

- vyhodnocení úspěšnosti přenosu a zpracování importních datových souborů od jednotlivých subjektů zúčtování
- prověření integrity dat
- kontrola návaznosti jednotlivých transakcí s elektronickou peněženkou
- kontrola původu vstupních dat
- kontrola souladu systému s legislativou (hlídání stanovených limitů)

### 3.1.7. Vybavení modelového Zúčtovacího centra multifunkční čipové karty

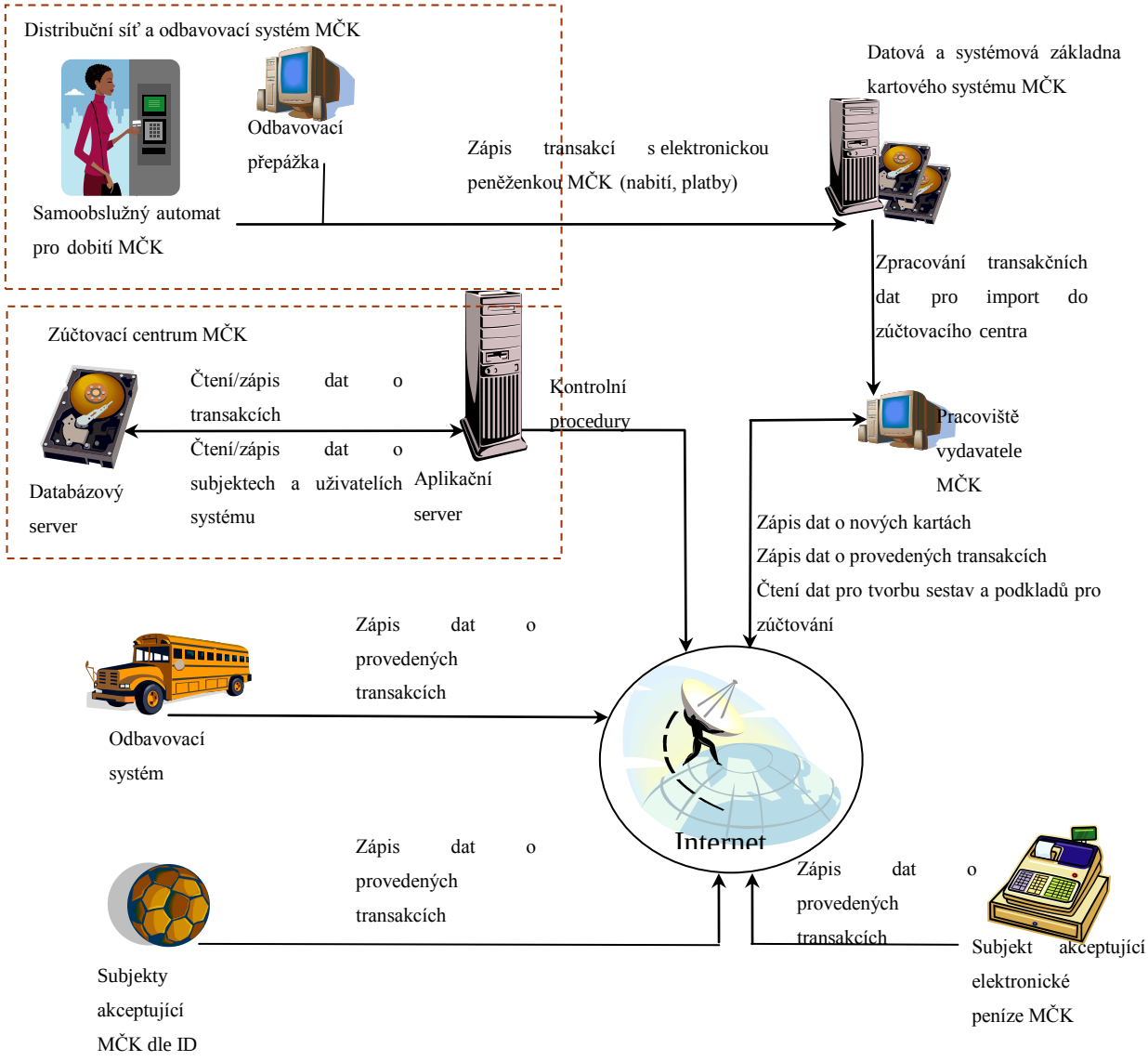
- aplikační server
- HW – výkonný server
- operační systém
- aplikační SW
- databázový server
- HW – výkonný server s kvalitním zálohovacím zařízením
- operační systém
- databázový systém
- zálohovací systém

Z důvodu zabezpečení proti ztrátě dat může být i u Zúčtovacího centra systému multifunkční čipové karty vybudována redundantní replikace dat na sekundární datový server. Vzhledem k tomu, že veškerá data do centra budou dodávána jednotlivými subjekty ve formě importních souborů, není tento systém tak náchylný ke ztrátě dat, jako odbavovací systém a Kartové centrum, a tedy duplicita dat není pro takový systém nezbytná.

### 3.1.8. Zúčtování předplatních kuponů

Pro přesnější rozdělení tržeb z prodeje předplatních kuponů – časových jízdenek - mezi jednotlivé dopravce může být zúčtovacím centrem vyhodnocováno i využívání těchto jízdenek. Zavedení tohoto způsobu rozdělování tržeb závisí na dohodnutém tarifním systému a na sjednaných smlouvách mezi dopravci a koordinátory integrovaných dopravních systémů. Samozřejmě se zde zúčtují i platby z elektronické peněženky.

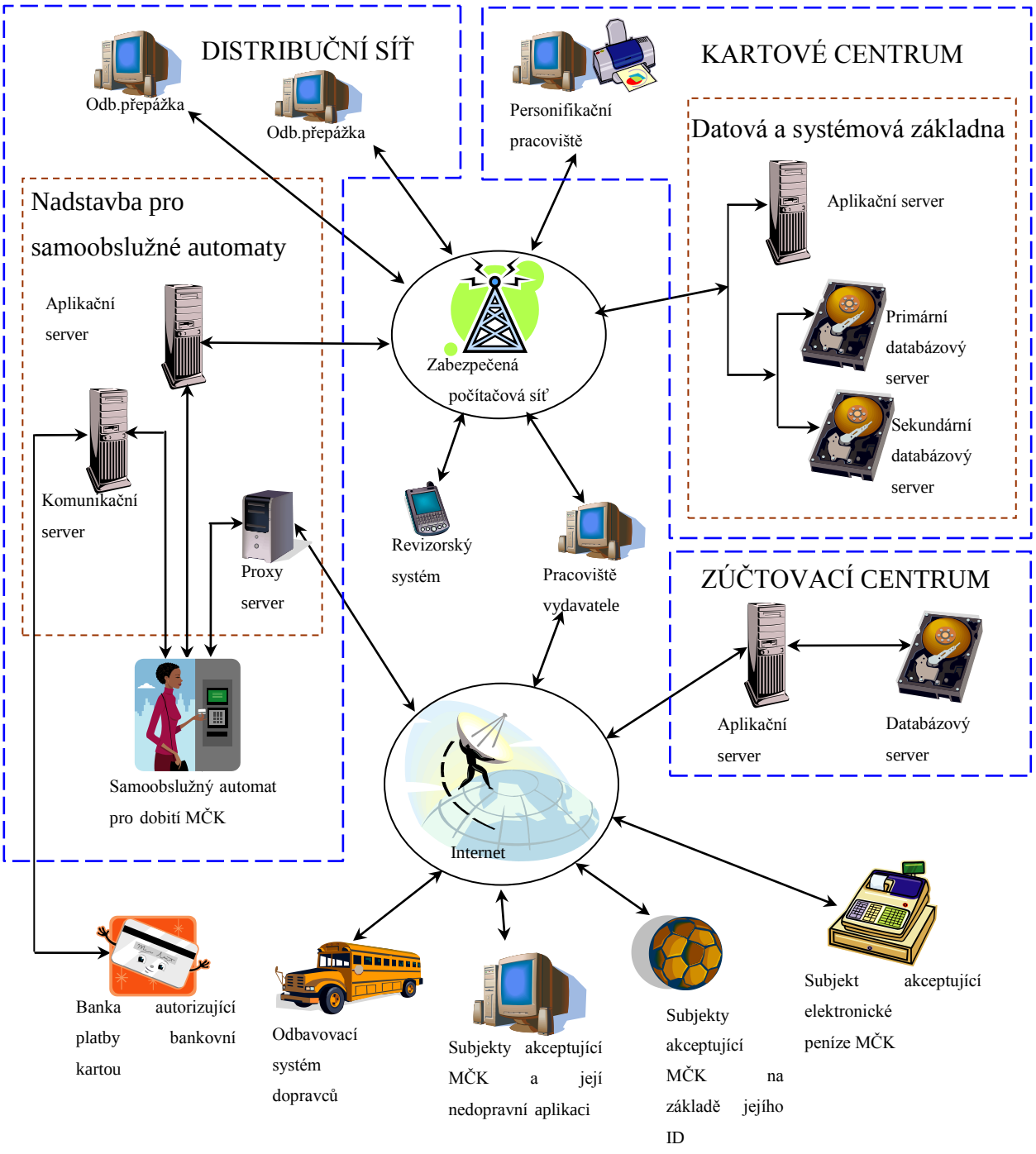
Obrázek 3 Schéma zúčtování v systému multifunkční čipové karty (11)




### 3.1.9. Celkové schéma modelového systému městské čipové karty

Toto schéma znázorňuje celkový model systému městské čipové karty. Pro zajímavost je do něj vřazeno i schéma funkce dobíjení multifunkčních čipových karet v samoobslužných automatech pomocí bankovní karty s její autorizací např. přes Global Payment prostřednictvím jedné smluvní banky.

Obrázek 4 Schéma celkového řešení systému městské čipové karty (11)



### 3.1.10. Modelový případ rozložení aplikací na MČK

Tabulka je příkladem možného rozdělení aplikací v datovém prostoru MČK. Cílem je upřesnit, jaká data bývají na čipové karty ukládána, vzhledem k tomu, že hrozí (a bylo již prokázáno) že data z těchto karet lze po prolomení přístupových klíčů neoprávněně vyčíst. Pro příklad je použita karta MIFARE standard 1kBYTE se strukturou MAD.

Tabulka 1 Modelové rozložení aplikací na městské čipové kartě (11)

| Číslo sektoru | Číslo bloku | Popis | Klíče |
|---|---|---|---|
| 0. | 0 | Sériové číslo karty, kód výrobce a další doplňující údaje. | A0, B0 |
| | 1,2 | MAD Struktura (mapa rozmístění aplikací do sektorů na | |
| 1. | 0,1,2 | Údaje o držiteli karty | A1, B1 |
| 2. | 0,1,2 | Aplikace abonentní předplatné<br>1. Kupón | A2, B2 |
| 3. | 0,1,2 | Aplikace abonentní předplatné<br>2. Kupón | A2, B2 |
| 4. | 0,1,2 | Aplikace elektronická peněženka<br>(1. sektor) | A3, B3 |
| 5. | 0,1,2 | Aplikace elektronická peněženka<br>(2. sektor) | A3, B3 |
| 6. | 0,1,2 | Aplikace elektronická peněženka<br>(3. Sektor) | A3, B3 |
| 7. | 0,1,2 | Aplikace elektronická peněženka<br>(4. Sektor) | A3, B3 |
| 8. | 0,1,2 | Aplikace předplatné v MHD<br>3. Kupón | A4, B4 |
| 9. | 0,1,2 | Aplikace předplatné v MHD<br>4. Kupón | A4, B4 |
| 10. | 0,1,2 | Aplikace předplatné integrovaného dopravního systému<br>5. Kupón | A5, B5 |
| 11. | 0,1,2 | Aplikace předplatné integrovaného dopravního systému<br>6. Kupón | A5, B5 |
| 12. | 0,1,2 | Volné místo | A20, B20 |
| 13. | 0,1,2 | Volné místo | A20, B20 |
| 14. | 0,1,2 | Volné místo | A20, B20 |
| 15. | 0,1,2 | Volné místo | A20, B20 |

V nultém a prvním sektoru pak mohou být uloženy například tyto údaje:

1. Jedinečné ID karty
2. Jedinečné ID vydavatele karty
3. Jméno a příjmení držitele karty
4. Datum narození držitele karty
5. Jedinečné ID jednotlivých aplikací
6. Platnost karty
7. Jednoznačná Identifikace rozlišení typu karty

Aplikace elektronická peněženka pak může obsahovat například tato data:

1. Aktuální stav peněženky
2. Log obsahující čtyři poslední transakce
3. Záloha elektronické peněženky

Aplikace abonentní předplatné pak může obsahovat například tato data:

1. Označení např. divadla pro které předplatné platí
2. Datum od kdy předplatné platí
3. Datum do kdy předplatné platí
4. Typ předplatného (plnocenné, dětské, důchodce atp.)
6. Na této modelové kartě mohou být uložena dvě taková předplatná

Aplikace předplatné MHD pak může obsahovat například tato data:

1. Označení zóny (územní platnost)
2. Datum od kdy předplatné platí
3. Datum do kdy předplatné platí
4. Typ předplatného (plnocenné, dětské, důchodce atp.)
5. Typ předplatného (jednoznačné ID tarifu neboli předplatného)
6. Na této modelové kartě mohou být uložena dvě taková předplatná s různými daty platnosti a různou územní platností

Aplikace předplatné integrovaného dopravního systému pak může obsahovat například tato data:

1. Označení zóny (územní platnost)

2. Datum od kdy předplatné platí

3. Datum do kdy předplatné platí

4. Typ předplatného (plnocenné, dětské, důchodce atp.)

5. Typ předplatného (jednoznačné ID tarifu neboli předplatného)

6. Na této modelové kartě mohou být uložena dvě taková předplatná s různými daty platnosti a různou územní platností

# 4. Volba bezpečnostního modelu projektu multifunkčních čipových karet

## 4.1. Zjištění rozdílů mezi systémy z pohledu bezpečnosti

Pokud chceme zjistit základní rozdíly mezi systémy multifunkčních karet a běžnými informačními systémy (od tohoto zjištění se odvíjí syntéza, proč přenesená bezpečnostní pravidla nefungují), seřaďme základní bezpečnostní zjištěné atributy v předchozích kapitolách popsaných systémů do tabulky k porovnání. Pro hodnocení atributů je použita následná škála od jedné do pěti.

1. atribut se prakticky nevyskytuje
2. atribut má nízkou hodnotu – zanedbatelná míra rizika
3. atribut má střední hodnotu – střední míra rizika
4. atribut je nadprůměrný – nadprůměrná míra rizika
5. atribut se vyskytuje v maximální možné míře – riziko je velmi vysoké

Hodnoty v tabulce tvoří průměr ze získaných údajů. O vyplnění tabulky pro svůj systém byli požádáni tři správci podnikových informačních systémů, v případě multifunkční čipové karty pocházejí zjištěná data od jednoho správce systému multifunkční karty, jednoho projektového manažera zabývajícího se dodávkami těchto systémů a jednoho bezpečnostního konzultanta poskytujícího služby i systémům multifunkčních karet.

Tabulka 2 – Vlastnosti informačních systémů z pohledu bezpečnosti

| Název atributu | Běžný IT systém | Systém MČK |
|---|---|---|
| Míra outsourcingu | 1-3 | 3-5 |
| Zpracování osobních údajů vlastních subjektů (zaměstnanců) | 5 | 3 |
| Zpracování citlivých osobních údajů vlastních subjektů (zaměstnanců) | 4 | 3 |
| Zpracování osobních údajů cizích subjektů | 1-2 | 5 |
| Zpracování citlivých osobních údajů cizích subjektů | 1 | 3-4 |
| Využívání systému třetími (smluvními) subjekty | 1 | 4-5 |
| Zpracovávaná data o vlastním majetku | 5 | 3-5 |
| Zpracovávaná data o cizím majetku | 1-2 | 4-5 |
| Riziko napadení systému zvenčí | 3 | 5 |
| Využití přístupu přes internet k datům v systému | 1-2 | 3-4 |
| Využívání cizí infrastruktury | 1-3 | 3-5 |
| Rozvoj systému o další aplikace | 1-3 | 4-5 |

Z tabulky č. 2 plyne, že hlavní rozdíl mezi srovnávanými systémy je v míře zpracovávaných dat cizích subjektů a o cizích subjektech. Systém MČK využívá ve větší míře i outsourcovaných prostředků. Dále z principu věci velmi často smluvní partneři MČK využívají přístup k datům přes internet. Stejně lze vnímat i motivaci k napadení systému zvenčí. Pokud se hacker rozhoduje pro útok, motivaci má buď finanční, nebo útok uskutečňuje pro svoji prestiž. V obou případech je pak pro něj atraktivnější zvolit systém MČK. Z pohledu ekonomického zisku je to snaha o pozměnění dat na kartách nebo v systému pro vlastní prospěch (dobití elektronické peněženky, prodloužení platnosti předplatného, získání vstupenek na koncert). U podnikového systému mohu uvažovat odeslání částky z firemních účtů na vlastní, získání know-how, nicméně všechny tyto důvody naleznu i u systému MČK.

## 4.2. Volba bezpečnostního modelu

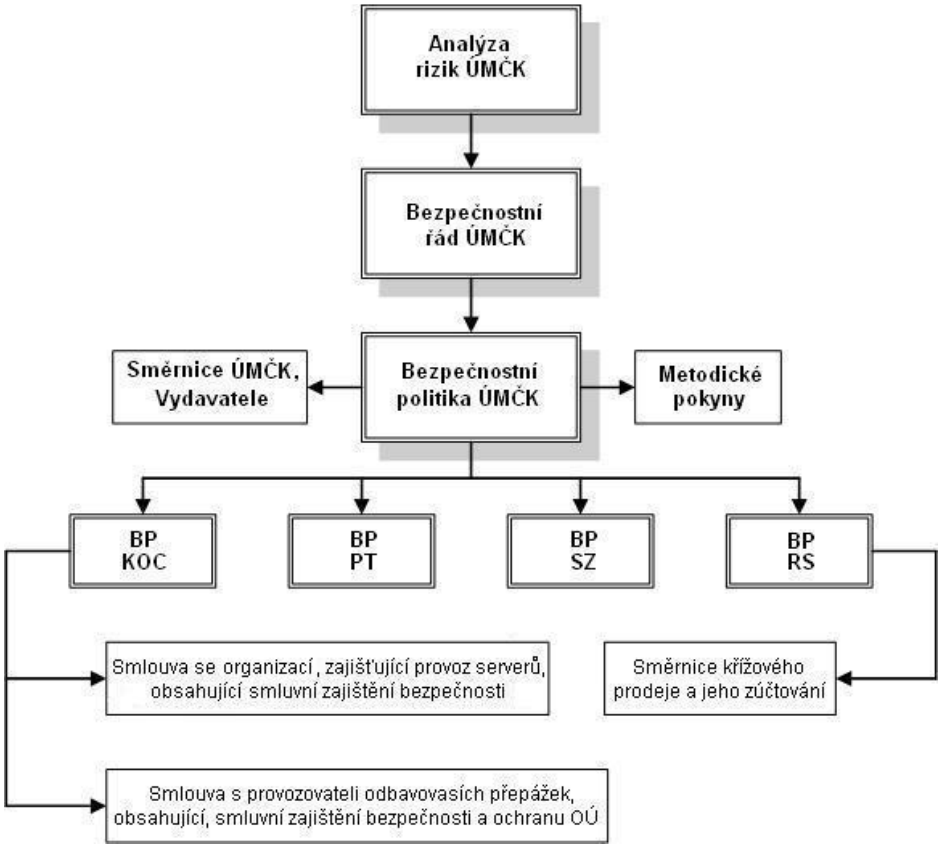
Pro volbu bezpečnostního modelu (struktury dokumentace) je třeba vzít v úvahu takto definované rozdíly. V systému MČK tedy musím daleko více ošetřit bezpečnostní rizika plynoucí z takto nalezených rozdílů. Obvykle používaná bezpečnostní dokumentace zpravidla řeší bezpečnost vlastního systému, velmi slabě je však v bezpečnostních dokumentech ošetřena bezpečnost v outsourcovaných částech.

Pokud tedy mám vytvořit bezpečnostní dokumentaci nad systémem MČK, který se vyznačuje velkou mírou přístupu k IT prostředkům z vnějšku systému, je třeba ošetřit rizika z toho plynoucí, v míře těmto rizikům odpovídající. Jedna z nejpoužívanějších praktik k docílení bezpečnosti je bezpečnost technická. Takový typ opatření úspěšně nasazujeme na IT prostředcích, které máme pod vlastní správou. Zde se však dostávám do situace, kdy technické prostředky, kterými je k systému přistupováno, pod vlastní správou nemám. Nabízí se tedy možnost uložit těmto subjektům (přistupujícím k mým datům) požadavky na technickou bezpečnost. Subjekt ovšem musí takové požadavky akceptovat, správce MČK pak by měl jejich nasazení pravidelně kontrolovat. Při velkém množství subjektů je však taková varianta z praktického hlediska neproveditelná. Pro účel tvorby bezpečnostní dokumentace pak zbývá použít smluvní zajištění vůči takovým třetím subjektům. Jedná se vlastně o smluvní přesunutí rizika na takovou třetí stranu. Vzhledem k vymahatelnosti takového smluvního zajištění je nutné využít pro tvorbu vztahu služeb odborníků, tedy právní kanceláře. Taková povinnost pak musí být uložena právě v bezpečnostní dokumentaci systému MČK.

Dalším významným rozdílem, který lze mezi systémy najít, a je velmi důležitý pro volbu modelu, je dynamický až překotný rozvoj u systému MČK. Podnikový IT systém je z pohledu vývoje poměrně stabilní, jeden druh aplikace je nahrazen jiným prakticky se stejnou funkcí, v případě sofistikovaných ERP systémů pak je pouze rozšiřován o další moduly. Naprostá většina inovací se pak děje na vlastní infrastruktuře, k její masivní změně dochází spíše výjimečně. Systém MČK se chová jinak. Pokud vezmeme velmi jednoduchý případ nové akceptace MČK jako knihovního průkazu, dostává se řešitel do následující situace. Součástí řešení bude přečtení jména držitele karty z čipu karty, dále pak odečet elektronické hotovosti z čipu karty za služby poskytnuté čtenáři. IT oddělení knihovny je tedy třeba nějakým způsobem předat čtecí klíče ke kartám. Tyto klíče je nutné v informačním systému knihovny zabezpečit proti zneužití. Knihovna dále musí obdržet zařízení a příslušný software k práci s elektronickou peněženkou. Musí být schopna hotovost nejen odečíst, ale příslušně pracovat

s účetními sestavami s tím spojenými. Dále musí data o odečtech odesílat pravidelně do zúčtovacího centra a pomocí příslušného softwaru si nad tímto mechanismem udržet i přehled. Pokud nyní situaci vyhodnotíme z bezpečnostního hlediska, informační systém knihovny pracuje s mnoha údaji poskytovanými systémem MČK, s tím, že poskytované (zpracovávané ) údaje jsou z pohledu bezpečnosti MČK velmi rizikové. Ošetřit takové údaje přímo vlastní bezpečnostní dokumentací MČK je velmi obtížné. Nových rizik a situací je tolik, že to znamená přepracovat bezpečnostní dokumentaci v tradiční struktuře prakticky od základu a to vždy při začlenění nového projektu. Pokud bychom akceptovali takovou cestu, získáme poměrně velmi brzo obrovský balík bezpečnostní dokumentace, která je přehledná s velkými obtížemi. Pokud budeme uvažovat každoroční revizi dokumentace, řešíme další vážný problém. Nové projekty řeší různí lidé a různé projektové týmy. Ti pak nechápou, proč byly některé změny v celkovém balíku dokumentace učiněny a hlavně ztrácí přehled o souvislostech. Je tedy třeba zvolit odlišné schéma tvorby bezpečnostní dokumentace. Jako vhodnou možnost vidím zvolit model, kdy nahoře budou tři relativně obecné bezpečnostní dokumenty, které budou stanovovat požadavky na podřízenou dokumentaci. Vrcholové dokumenty pak jsou jakýmisi katalogy, které nastaví požadovanou míru bezpečnosti a konkrétní bezpečnost pak budou řešit konkrétní bezpečnostní dokumenty jednotlivých dílčích projektů. Tato úprava zajišťuje přehlednost dokumentace a odstraňuje zaplevelování takové dokumentace požadavky, které vycházejí z dílčích projektů a jejich podmínek, ale není důvod tímto způsobem řešit jiné dílčí projekty za zcela odlišných podmínek. Model, který byl vytvořen na základě zjištěných poznatků, je znázorněn na obrázku číslo pět. Podřízené dokumenty jsou „Bezpečnostní projekty“, které řeší již konkrétní provedení zabezpečení u jednotlivého projektu, v závislosti na jeho technickém a organizačním provedení. Dále přistupuje ostatní dokumentace, jako jsou směrnice, metodiky, smlouvy. I tyto dokumenty jsou vytvářeny v souladu s požadavky nastavenými vrcholovou dokumentací.

Obr č. 5 -Model bezpečnostní dokumentace ISMČK




Poté, co jsem takto definoval rozdíly, na jejich základě vybral bezpečnostní model, lze přikročit přímo k tvorbě takové vzorové dokumentace. Bezpečnostní model bude zapracován i do vzorové dokumentace.

# 5. Zpracování vzorového bezpečnostního modelu projektu multifunkční čipové karty.

Vzorový bezpečnostní model obsahuje tři vrcholové bezpečnostní dokumenty a to Analýzu rizik, Bezpečnostní řád a Bezpečnostní politiku. V těchto dokumentech jsou zároveň

nastavena základní pravidla pro vznik podřízené bezpečnostní dokumentace a pravidelnou revizi celého modelu.

## 5.1. Analýza rizik

Analýza rizik je nezbytným krokem systémového řešení bezpečnosti. Je možno ji provádět pro celou organizaci nebo jen informační systém, samostatně nebo před zpracováním plánů kontinuity, jak organizace, tak informačního systému. V rámci životního cyklu informačního systému většinou předchází vytvoření Bezpečnostní politiky. Měla by být opakována nebo aktualizována při každé změně ohrožení nebo zabezpečení.

Analýza rizik představuje proces, který pomáhá odhalit bezpečnostní rizika působící na organizaci nebo informační systém a přispívá ke zkvalitnění návrhu bezpečnostních opatření. V prvním kroku se provádí hodnocení bezpečnostních rizik, které představuje identifikaci aktiv a hrozeb. V dalším kroku se hodnotí zranitelnost aktiv vůči těmto hrozbám a pravděpodobnost jejich výskytu. V rámci hodnocení bezpečnostních rizik se také provádí odhad jejich potenciálního dopadu. Na základě výsledků hodnocení bezpečnostních rizik se navrhují bezpečnostní požadavky pro systém, které mají zajistit bezpečný provoz a využívání informačních systémů.

Cílem analýzy rizik je identifikovat rizika a nalézt slabá místa ISMČK z hlediska bezpečnosti a stanovit jejich pravděpodobnost výskytu. Analýza rizik se v rámci tohoto dokumentu omezuje na tyto oblasti:

- Prodejní a provozní místa
- Serverovny
- Komunikace
- Karty

Analýza rizik musí procházet pravidelnou aktualizací, a to s frekvencí 1x do roka, při výskytu bezpečnostního incidentu a vždy při realizaci nového projektu v rámci ISMČK

### 5.1.1. Aktiva

V rámci tohoto projektu jsou definována následující aktiva:

- peníze
- transakce a data
- kryptografické klíče
- osobní údaje

### 5.1.2. Výskyt jednotlivých aktiv v prostředí ÚMČK

- aktivum peníze:
    - pracoviště pro prodej kuponů nabíjení EP
    - pokladna pro úhradu pokut z přepravy
    - pracoviště reklamací
- aktivum transakce a data:
    - pracoviště pro prodej kuponů a nabíjení EP
    - servery
    - komunikační linky
    - pracoviště administrátorů aplikace
    - revizorské čtečky
    - mobilní terminály (ruční platební terminály MČK, terminály ve vozidlech)
    - zařízení pro akceptaci MČK mimo vlastnictví ÚMČK
- aktivum kryptografické klíče
    - pracoviště pro prodej kuponů a nabíjení EP
    - pokladna pro úhradu pokut z přepravy
    - pracoviště reklamací
    - revizorské čtečky
    - mobilní terminály (ruční platební terminály MČK, terminály ve vozidlech)
    - pracoviště pro generování kryptografických klíčů
    - zařízení pro akceptaci MČK mimo vlastnictví ÚMČK
    - čipové karty
    - servery
    - komunikační linky
- aktivum osobní údaje
    - pracoviště pro prodej kuponů a nabíjení EP
    - pracoviště výroby MČK
    - pracoviště reklamací
    - zařízení pro akceptaci MČK mimo vlastnictví ÚMČK
    - mobilní terminály (ruční platební terminály MČK, terminály ve vozidlech)

### 5.1.3. Definovaná rizika

- pro aktivum peníze

    - zcizení tržby nebo její části vlastními zaměstnanci
    - krádež tržby při převozu
    - přepadení a loupež
    - podvodné jednání (hlavně na pokladně pro úhradu pokut z přepravy)
- pro aktivum transakce
    - ztráta transakcí a dat vinou nefunkčnosti systému
    - ztráta transakcí a dat vinou přerušení komunikačních linek
    - ztráta transakcí a dat vinou poruchy pracovní stanice
    - ztráta transakcí a dat vinou poruchy serveru
    - ztráta transakcí a dat vinou úmyslného vymazání transakcí
    - ztráta nebo změna transakcí a dat vinou úmyslného průniku do sítě
- pro aktivum kryptografické klíče
    - prozrazení kryptografických klíčů
    - krádež revizorské čtečky
    - krádež čtečky karet na kontaktním místě
    - krádež karetního terminálu (z vozidla MHD, popř. ze skladu)
    - ztráta, krádež SAM
- pro aktivum osobní údaje
    - ztráta žádosti
    - zcizení žádosti
    - okopírování žádosti a „vynesení“ mimo Vydavatele
    - neoprávněné vyčtení OÚ z MČK
    - stažení OÚ z DB ISMČK
    - přečtení OÚ z displeje mobilních terminálů
- všeobecná
    - požár
    - povodeň
    - selhání dodávky energie
    - personální
    - napadení ISMČK škodlivým SW
    - sociální inženýrství
    - nedostatečné smluvní zajištění

### 5.1.4. Hodnocení a eliminace rizik

Hodnocením rizik může být pověřen i nezávislý subjekt. Hodnocení rizik se bude týkat celého ISMČK. ÚMČK provede hodnocení rizik při každé významné změně v systému. ÚMČK bude pravidelně provádět bezpečnostní audit ISMČK (min. 1x ročně). Na základě hodnocení rizik budou určeny odpovídající bezpečnostní protiopatření, potřebné k ochraně proti možným negativním incidentům v oblasti důvěrnosti, integritě dat a dostupnosti služby.

Tabulka 3 - Legenda: Pravděpodobnost výskytu rizika

| | Hodnota | Popis | Výskyt |
|---|---|---|---|
| **1.** | **častý výskyt** | pravděpodobný, často se vyskytující výskyt | 1x nebo vícekrát za rok |
| **2.** | **pravděpodobný výskyt** | událost vznikne několikrát v průběhu daného období, jedná se o časté ohrožení | 1x za 3 roky |
| **3.** | **příležitostný výskyt** | událost vznikne jen někdy v průběhu daného období, | 1x za 10 let |

| | | | |
|---|---|---|---|
| | | zřídkavé ohrožení, jedná se spíše o náhodný výskyt | |
| **4.** | **málo pravděpodobný výskyt** | výskyt nežádoucí události je zcela ojedinělý | 1x za 20 let |
| **5.** | **nepravděpodobný výskyt** | vznik události je téměř nemožný a může nastat za předpokladu souběhu několika málo pravděpod. výskytů | 1x za 50 let |

O ohodnocení rizik byla požádána stejná skupina subjektů, jako v prvním případě v tabulce č.2.

Pravděpodobnost rizika je opět stanovena průměrem ze zjištěných hodnot. Zajímavostí jistě je, že zadáním pro vyplnění bylo použít pokud možno jako zdroj údajů záznam o incidentech, pokud se námi definované riziko v dané organizaci objevuje. Takový auditní záznam vytváříme vlastně proto, abychom později věděli, co se v průběhu práce v systému dělo. Je to vlastně protokol, který zkoumáme po bezpečnostním incidentu. (13) Záznamy o incidentech jsou však zpravidla v organizacích vedeny až za poslední dva, tři roky, (zřejmě důsledek růstu povědomí o počítačové bezpečnosti), pro rizika, jež se tedy v daném časovém období v existujících záznamech neobjevily, byl použit expertní odhad vycházející v podstatě z paměti dotazovaných.

### 5.1.5. Aktivum Peníze

Tabulka 4 – Aktivum peníze

| Aktivum | Riziko | Pravděpod. výskytu rizika | Dopady | Eliminace rizika | Náprava | |
|---|---|---|---|---|---|---|
| | | | | | Co dělat, když nastane | Kdo provede |
| Peníze | Zcizení tržby nebo její části vlastními zaměstnanci | 4 | | definováno v interních předpisech Vydavatele | definováno v interních předpisech Vydavatele | |
| | Krádež tržby při převozu | 4 | | definováno v interních předpisech Vydavatele | definováno v interních předpisech | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | Vydavatele | |
| | Přepadení a loupež | 4 | | definováno v interních předpisech Vydavatele | definováno v interních předpisech Vydavatele | |
| | Podvodné jednání | 3 | | definováno v interních předpisech Vydavatele | definováno v interních předpisech Vydavatele | |
| | Nefunkčnost systému z technických důvodů | 1 | Snížení tržeb z MČK | Důsledná a pravidelná kontrola ISMČK a dodržování předepsaných postupů při práci s ISMČK | Doplnění HW a SW infrastruktury o prvky, zvyšující spolehlivost ISMČK | |

### 5.1.6. Aktivum Transakce a data

Tabulka 5 – Aktivum Transakce a data

| Aktivum | Riziko | Pravděpod. výskytu rizika | Dopady | Eliminace rizika | Náprava | |
|---|---|---|---|---|---|---|
| | | | | | Co dělat, když nastane | Kdo provede |
| Transakce a data | Ztráta transakcí a dat vinou nefunkčnosti systému | 2 | ○ V ISMČK chybějí transakce<br>○ reklamace a stížnosti cestujících | ○ kvalitní otestování aplikace<br>○ prvotní výběr vhodných technických prostředků | ○ detekce příčiny selhání aplikace<br>○ programové úpravy k zamezení nefunkčnosti ISMČK<br>○ důkladné testování aplikace | Správce ISMČK |
| | Ztráta transakcí a dat vinou přerušení komunikačních linek | 2 | ○ V ISMČK chybějí transakce<br>○ reklamace a stížnosti cestujících | ○ instalace kvalitních síťových prvků<br>○ zabezpečení komunikací proti odposlechu a výpadku<br>○ zvýšený dohled nad pracemi v blízkosti komunikačních linek | ○ detekce příčiny selhání komunikace<br>○ přechod aplikace ISMČK do autonomního režimu<br>○ oprava síťového spojení | Správce sítě, ISMČK |
| | Ztráta transakcí a dat vinou poruchy pracovní stanice | 2 | ○ V ISMČK chybějí transakce<br>○ reklamace a stížnosti cestujících<br>○ přerušení práce na prodejních místech | ○ instalace kvalitních pracovních stanic<br>○ správné nastavení OS pracovní stanice<br>○ správné nastavení aplikace ISMČK na pracovní stanici<br>○ správné nastavení a připojení periférií k pracovní stanici<br>○ záložní pracovní stanice se stejnými parametry | ○ detekce příčiny selhání pracovní stanice<br>○ výměna pracovní stanice za funkční, nebo<br>○ oprava pracovní stanice na místě | Správce ISMČK |
| | Ztráta transakcí a dat vinou | 4 | Při poruše serverů a | definováno v interních předpisech smluvního | definováno v interních | Správce ISMČK |

| | | | | | | |
|---|---|---|---|---|---|---|
| | poruchy serveru nebo diskového pole | | diskových polí najednou bude nutné konsolidovat transakce | partnera poskytujícího službu (správa serverů, OS a zálohování) | předpisech smluvního partnera poskytujícího službu | |
| | Ztráta transakcí a dat vinou úmyslného vymazání transakcí | 4 | V ISMČK chybí transakce | ○ nastavení aplikace tak, aby byla schopná detekovat chybějící transakce<br>○ kontrola transakčních logů<br>○ personální obsazení pozice správce serverů (kvalifikace, spolehlivost) | ○ zjištění chybějících transakcí<br>○ obnovení chybějících transakcí ze zálohy | Správce ISMČK |
| | Ztráta nebo změna transakcí a dat vinou úmyslného průniku do uzavřené VPN síťě | 3 | V ISMČK chybí nebo jsou změněny transakce | ○ nastavení komunikačních linek dle požadovaých parametrů ISMČK<br>○ kontinuální monitorig chodu sítě | ○ kontrola nastavení síťových prvků<br>○ analýza příčin<br>○ úprava nastavení komunikačních linek<br>○ obnova dat ze zálohy | Správce sítě, ISMČK |

### 5.1.7. Aktivum Kryptografické klíče

Tabulka 6 – Aktivum Kryptografické klíče

| Aktivum | Riziko | Pravděpod. výskytu rizika | Dopady | Eliminace rizika | Náprava | |
|---|---|---|---|---|---|---|
| | | | | | Co dělat, když nastane | Kdo provede |
| Kryptografické klíče | Prozrazení kryptografických klíčů | 4 | ○ Mediální<br>○ Ztráta důvěry veřejnosti v systém | ○ Uložení kryptografickch klíčů v aplikaci tak, aby nebylo možné je v žádném případě přečíst<br>○ Uložení kryptografickýc h klíčů pouze v zašifrované podobě<br>○ Uložení klíčů v tištěné podobě v trezoru s jasně definovaným přístupem | ○ Úprava příslušného SW tak, aby bylo možné odhalit podvodné jednání<br>○ Úprava systému kryptografický ch klíčů na systém diverzifikovan ých klíčů | ÚMČK |
| | Krádež nebo ztráta mobilní čtečky | 2 | ○ Finanční ztráta za zařízení | ○ Protokolární svěření mobilní čtečky pracovníkovi<br>○ Hmotná zodpovědnost za mobilní čtečku<br>○ Nošení a používání zařízení tak, aby riziko nemohlo nastat | ○ Okamžité nahlášení incidentu vedoucímu pracovníkovi a POB, ÚMČK | Příslušný zaměstnanec<br>Příslušný nadřízený zaměstnance<br>POB, ÚMČK |
| | Krádež nebo ztráta stolní čtečky | 3 | ○ Finanční ztráta za zařízení | ○ Objektová bezpečnost pro kontaktní místa dle standardu Vydavatele | ○ Nahlášení incidentu vedoucímu pracovníkovi a POB, ÚMČK | Příslušný zaměstnanec<br>Přímý nadřízený zaměstnance<br>POB, ÚMČK |
| | Zcizení karetního terminálu ve vozidle | 4 | ○ Finanční ztráta za zařízení | ○ Umístění náhradních karetních terminálů v uzamčeném a zabezpečeném skladu<br>○ Upevnění karetního terminálu ve vozidle tak, aby nebylo možné jeho sejmutí bez speciálního nářadí | ○ Pořízení nového karetního terminálu<br>○ Aktivace karetního terminálu | POB, ÚMČK |
| | Ztráta nebo zcizení SAM | 2 | ○ Riziko vyčtení kryptografick ých klíčů ze SAM | ○ Uložení kryptografickýc h klíčů v SAM tak, aby nebylo možné je v žádném případě přečíst<br>○ Uložení | ○ Zablokování příslušného SAM v aplikaci<br>○ Umístění zablokovaného SAM na blacklist SAM | ÚMČK |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | kryptografickýc h klíčů pouze v zašifrované podobě<br>o Uložení prázdných i nahraných SAM v trezoru s jasně definovaným přístupem | | |

### 5.1.8. Aktivum Osobní údaje

Tabulka 7 – Aktivum Osobní údaje

| Aktivum | Riziko | Pravděpod. výskytu rizika | Dopady | Eliminace rizika | Náprava | |
|---|---|---|---|---|---|---|
| | | | | | Co dělat, když nastane | Kdo provede |
| Osobní údaje | Ztráta žádosti | 2 | o Mediální<br>o Ztráta důvěry veřejnosti v MČK | o Dodržování předepsaných postupů při manipulaci se žádostmi<br>o Uložení přijatých žádostí v předepsané formě na určené zabezpečené místo | o Nutnost požádat klienta o nové vyplnění žádosti | Příslušný zaměstnanec |
| | Zcizení žádostí | 4 | o Mediální<br>o Ztráta důvěry veřejnosti v systém | o Uložení žádosti v předepsané formě na určené zabezpečené místo | o Nutnost požádat klienta o nové vyplnění žádosti<br>o Kontrola procesu manipulace se žádostmi a jejich uložení | Příslušný zaměstnanec |
| | Okopírování a následné „vynesení“ žádosti mimo Vydavatele | 4 | o Mediální<br>o Ztráta důvěry veřejnosti v systém | o Dodržování předepsaných postupů při manipulaci se žádostmi<br>o Uložení přijatých žádostí v předepsané formě na určené zabezpečené místo<br>o Objektová bezpečnost pro kontaktní místa dle standardu Vydavatele | o Nahlášení incidentu vedoucímu pracovníkovi, POB, ÚMČK, | Příslušný zaměstnanec Přímý nadřízený zaměstnance POB, ÚMČK |
| | Neoprávněné vyčtení OÚ z MČK | 2 | o Mediální<br>o Ztráta důvěry veřejnosti v systém | o Systém diverzifikovaných kryptografických klíčů | o Nahlášení incidentu vedoucímu pracovníkovi, POB, ÚMČK, | ÚMČK |
| | Stažení OÚ z DB ISMČK | 4 | o Mediální | o Zabezpečení HW a SW ISMČK tak, aby nebylo možné cokoliv nahrát na externí paměťové médium<br>o Zpřístupnění sestav z ISMČK s OÚ dle příslušných rolí | o Nahlášení incidentu vedoucímu pracovníkovi, POB, ÚMČK, | Přímý nadřízený zaměstnance POB, ÚMČK |
| | Přečtení OÚ z displeje mobilních | | | o SW musí být upraven tak, aby se OÚ na displejích nezobrazovaly (s výjimkou čísla karty) | | Dodavatel SW, HW |

| | | | | | | |
|---|---|---|---|---|---|---|
| | terminálů | | | | | |

### 5.1.9. Aktivum Všeobecné

Tabulka 8 – Aktivum Všeobecné

| Aktivum | Riziko | Pravděpod. výskytu rizika | Dopady | Eliminace rizika | Náprava | |
|---|---|---|---|---|---|---|
| | | | | | Co dělat, když nastane | Kdo provede |
| Všeobecně | Požár | 3 | ○ Přerušení fungování kontaktního místa<br>○ Zničení serveru a diskového pole<br>○ Zničení vybavení kontaktního místa | ○ Dodržování platných požárních předpisů a směrnic, a vybavení pracovišť odpovídajícím způsobem (EPS, hasící přístroje) | Obnova funkčnosti dle plánů obnovy systému ISMČK | Příslušní zaměstnanci |
| Všeobecně | Povodeň | 5 | ○ Zničení vybavení kontaktního místa<br>○ Přerušení fungování kontaktního místa | ○ Umístění kontaktních míst mimo zátopové území<br>○ Při hrozícím nebezpečí včasné přemístění HW do bezpečných prostorů | Obnova funkčnosti dle plánů obnovy ISMČK | Příslušní zaměstnanci |
| Všeobecně | Selhání dodávky energie | 1 | ○ Přerušení fungování kontaktního místa po dobu výpadku energie | ○ Vybavení všech PC, serverů a aktivních prvků sítě záložními zdroji energie na dobu alespoň 15 minut<br>○ Redundantní komunikační linky | Pracovní stanice:<br>○ dokončení započaté transakce<br>○ nesmí být započata jiná transakce<br>○ bezpečné vypnutí pracovní stanice<br>○ čekat na pokyny vedoucích pracovníků k zahájení činnosti po obnově dodávky energie | Uživatel ISMČK |
| | | | | | Servery: definováno v interních předpisech SITmP | Správce ISMČK |
| Všeobecně | Personální bezpečnost | 2 | ○ Časté reklamace cestujících<br>○ Snížení důvěry cestujících v MČK<br>○ Snížení akceptovatelnosti MČK cestujícími<br>○ Mediální | ○ Výběr kvalitních pracovníků na jednotlivé pozice<br>○ Prověření skupin uživatelů na trestní bezúhonnost (zaměstnanci, kteří pracují s osobními údaji a penězi)<br>○ Pravidelná provozní školení zaměstnanců (min. 1x za 2 roky)<br>○ Dostatečné | Definováno v interních předpisech Vydavatele | Dotčení vedoucí zaměstnanci |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | vyškolení a vycvičení pracovníků kontaktního místa a ostatních provozních pracovišť | | |
| Všeobecně | Napadení systému ISMČK škodlivým SW | 3 | definováno v interních předpisech Vydavatele | definováno v interních předpisech Vydavatele | definováno v interních předpisech Vydavatele | |
| Všeobecné | Sociální inženýrství | 3 | ○ Poskytnutí údajů hackerům<br>○ Snížení důvěry cestujících v MČK<br>○ Mediální | ○ Výběr kvalitních pracovníků na jednotlivé pozice<br>○ Prověření skupin uživatelů na trestní bezúhonnost (zaměstnanci, kteří pracují s osobními údaji a penězi)<br>○ Pravidelná provozní školení zaměstnanců (min. 1x za 2 roky) | ○ Disciplinární řízení s viníkem<br>○ Opatření k zamezení opakování incidentu (SW, HW) | POB, ÚMČK, GŘ |
| Všeobecné | Smlouvy | 2 | ○ Nedostatečně vydefinovaný obsah smlouvy<br>○ Nejasný předmět plnění smlouvy<br>○ Nereálné termíny a ceny za plnění smlouvy<br>○ Finanční ztráty<br>○ Ztráta dat<br>○ Manipulace s OÚ | ○ Vícestupňová kontrola připravovaných a uzavíraných smluv<br>○ Výběr spolehlivých a prověřených partnerů | ○ Zahájit jednání o změně smlouvy | ÚMČK, právník |

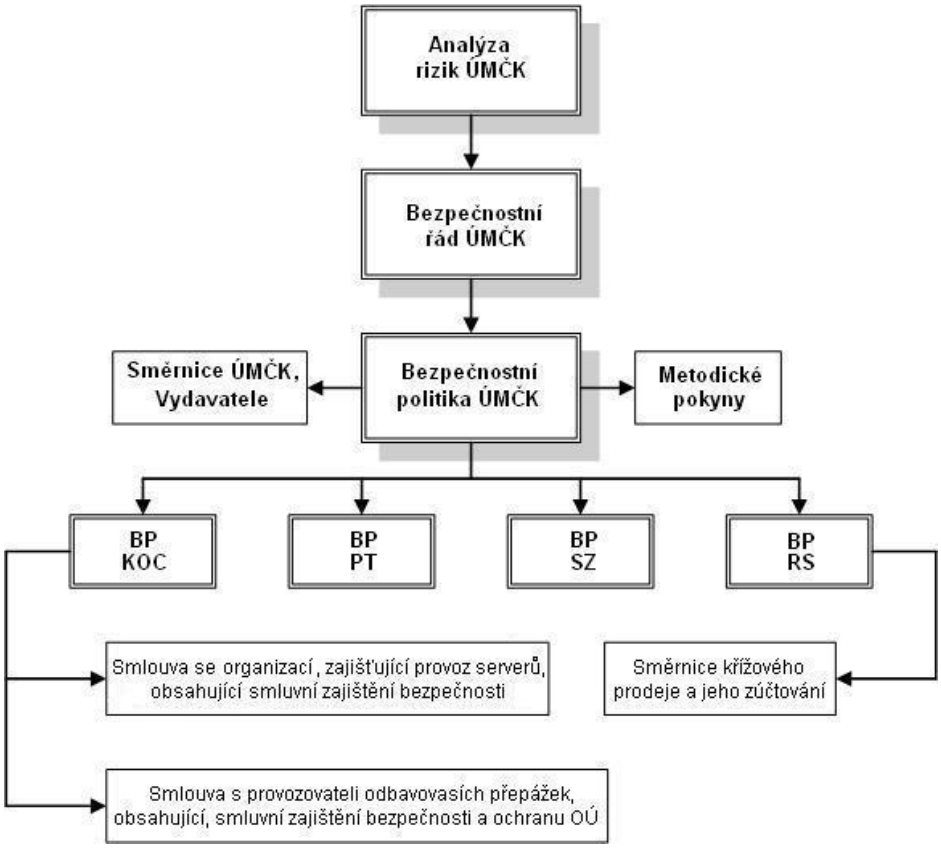
## 5.2. Bezpečnostní řád

### 5.2.1. Úvodní ustanovení

1. Bezpečnostní řád Úseku provozu MČK (dále jen ÚMČK) Organizace Vydavatele Multifunkční čipové karty (dále jen Vydavatel) je základním interním řídícím dokumentem pro oblast bezpečnosti ÚMČK.
2. Definuje pravidla k provedení dále uvedených zásad a v návaznosti na ostatní interní řídící dokumenty Vydavatel a ÚMČK definuje základní povinnosti a pravomoci zaměstnanců ÚMČK a dalších osob tak, aby se prosazování a dodržování těchto pravidel stalo nedílnou součástí plnění jejich povinností.
3. Bezpečnostní řád ÚMČK vychází z obecně platných závazných právních předpisů, hygienických předpisů, technických norem a předpisů pro zajištění bezpečnosti a ochrany zdraví při práci (BOZP), bezpečnosti informací a požární ochrany (PO).

### 5.2.2. Model bezpečnostní dokumentace

Obr č. 6 -Model bezpečnostní dokumentace ISMČK




1. Základní dokumenty na strategické úrovni jsou:

   - Analýza rizik – katalog rizik ÚMČK
   - Bezpečnostní řád – obecný dokument
   - Bezpečnostní politika informací - konkretizující dokument

2. Oba tyto dokumenty vycházejí z provedené Analýzy rizik.
3. Souběžně s ostatními strategickými dokumenty vzniká Havarijní plán.
4. Minimální náplň jednotlivých bezpečnostních dokumentů:
   a) Analýza rizik - obsahuje minimálně kapitoly:
      • Zpráva o aktivech
      • Definování hrozeb, jejich ohodnocení
      • Zpráva o analýze rizik
      • Prohlášení o aplikovatelnosti opatření
      • Plán zvládání rizik

b) Bezpečnostní řád - obsahuje minimálně kapitoly:
   • Působnost
   • Organizace bezpečnosti
   • Odpovědnost příslušných zaměstnanců
   • Personální bezpečnost
   • Fyzická bezpečnost

c) Bezpečnostní politika informací - obsahuje minimálně kapitoly:
   • Působnost
   • Východiska
   • Účel
   • Cíle bezpečnosti
   • Organizace bezpečnosti informací
   • Určení rolí
   • Aktiva
   • Evidence aktiv
   • Pravidla pro klasifikaci informací
   • Personální bezpečnost
   • Fyzická bezpečnost a bezpečnost prostředí
   • Zabezpečení zařízení
   • Správa informační a komunikační techniky, sítí a informačních systémů
   • Systém řízení přístupu
   • Vývoj a údržba IS
   • Dodržování zákonných norem

d) Provozní bezpečnostní dokumentace
   - Pro každý nový projekt vzniknou následné dokumenty (směrnice, metodické pokyny), které rozpracovávají dle potřeb jednotlivé konkrétní body bezpečnostní politiky.
   - Pokud nebude některé ustanovení všeobecné bezpečnosti aplikovatelné, musí být dokumentováno a řádně zdůvodněno
   - Pokud je projekt a jeho bezpečnost, nebo část projektu nebo bezpečnosti zabezpečena smluvně, řeší úroveň bezpečnosti druhá strana za stanovených sankcí při nedodržení předmětu smlouvy.
   - Některé projekty mohu mít směrnice, které jsou platné pouze pro daný projekt:
     - Systémová bezpečnostní politika.
     - Směrnice o klasifikaci informací a dat.
     - Směrnice o ochraně osobních údajů.
     - Směrnice o zvládání bezpečnostních incidentů.
     - Směrnice Zásady bezpečného ukládání, zálohování a archivace dat.
     - Směrnice Zásady řízení přístupu k informačnímu systému.
     - Metodický pokyn Osnova vzorové bezpečnostní příručky.

- Směrnice Zásady bezpečnosti využívání Internetu.
- Směrnice Zásady bezpečnosti provozu elektronické pošty.

e) Každý projekt pak bude mít svůj Bezpečnostní dokument projektu, který bude vycházet z Bezpečnostní politiky ÚMČK.

f) Vzhledem k různým použitým technologiím bude docházet k další konkretizaci příslušných dokumentů.

g) Každý dílčí bezpečnostní dokument převezme požadavky z nadřazené Bezpečnostní politiky, a doplní je o konkrétní požadavky, týkající se zejména použité technologie.

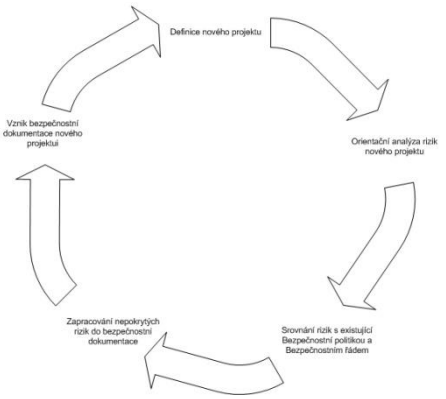
h) Existující bezpečnostní dokumentaci je nutné posoudit, zda odpovídá nadřazeným dokumentům.

i) Pokud bude do ISMČK připojen další projekt, je nutno vždy posoudit, zda odpovídá tomuto Bezpečnostnímu řádu a Bezpečnostní politice a zda nevnáší do projektu další, do té doby neošetřená rizika. Pokud se taková rizika objeví, jsou zapracována do celého systému bezpečnostní dokumentace.

j) Dokumenty mohou mít předepsanou náplň například i ve formě tabulek, nebo naopak může být některá kapitola dle potřeby rošířena do samostatného dokumentu

k) Cyklus vzniku bezpečnostní dokumentace nového projektu

Obr č. 7 – Cyklus vzniku bezpečnostní dokumentace nového projektu




### 5.2.3. Působnost

1. Pravidla bezpečnosti jsou platná pro všechny zaměstnance ÚMČK a dále pro zástupce externích subjektů a třetích stran, kteří spolupracují s ÚMČK, nebo se nacházejí v lokalitách a prostorách ÚMČK a u kterých vzniká potřeba tato bezpečnostní pravidla realizovat.
2. Pravidla bezpečnosti uvedená v tomto bezpečnostním řádu a v interních řídících dokumentech mohou být dále rozpracována v interních směrnicích ÚMČK. Takové směrnice jsou podřízeny tomuto řádu a navazujícím interním řídícím dokumentům ÚMČK a v některých případech Vydavatele MČK.

3. Cílem organizace bezpečnosti je vytvořit v rámci MČK takové vědomí potřeby bezpečnosti, které se stane neoddělitelnou součástí chodu ÚMČK a součástí celkové politiky v rámci Vydavatele.

### 5.2.4. Organizace bezpečnosti

1. Bezpečnost je nutné jednotně organizovat, prosazovat a řídit v rámci MČK, a při aktivní spolupráci všech zaměstnanců ÚMČK a zaměstnanců spolupracujících organizací.
2. Všichni zaměstnanci ÚMČK musí být poučeni o důsledcích porušení bezpečnostních předpisů.
3. Zástupci externích subjektů a třetích stran, kteří spolupracují anebo se nacházejí v lokalitách a prostorách ÚMČK a u kterých je potřeba realizovat tato bezpečnostní pravidla, musí být prokazatelně seznámeni s relevantními ustanoveními tohoto řádu, stejně tak jako s navazující interní řídící dokumentací. Dále musí být informováni o povinnostech, které je nutné v rámci spolupráce dodržovat.
4. Externí subjekty a třetí strany musí být informovány nejen o možných důsledcích porušení tohoto bezpečnostního řádu a ostatních navazujících předpisů, ale i o sankcích uložených za toto porušení.
5. Organizace jednotlivých oblastí bezpečnosti je definována v tomto řádu a upřesněna v navazujících interních řídících dokumentech.

### 5.2.5. Odpovědnosti

1. Odpovědnost jednotlivých zaměstnanců ÚMČK a zástupce externích subjektů a třetích stran, kteří spolupracují, nebo se nacházejí v lokalitách a prostorách MČK, vyplývá z příslušných ustanovení tohoto řádu a navazujících interních řídících dokumentů.
2. Každý zaměstnanec ÚMČK musí mít jen takové pravomoci a takové přístupy k informacím, jaké skutečně nezbytně potřebuje pro výkon své funkce. Tato pravidla musí být bez výjimky uplatňována zejména v oblasti ochrany osobních údajů a utajovaných skutečností.
3. Všichni zaměstnanci ÚMČK, u kterých dochází ke styku s informacemi, které by mohly ohrozit bezpečnost systému MČK, musí podepsat příslušná prohlášení o mlčenlivosti podle okruhu informací, se kterými se seznamují.
4. Statutární zástupce ÚMČK a vedoucí dalších pracovišť ÚMČK odpovídají zejména za:
    a) Ochranu všech aktiv.
    b) Účinné prosazování bezpečnostního řádu a bezpečnostních politik.
    c) Zvyšování bezpečnostního povědomí zaměstnanců.
    d) Definování aktiv, která mají být zabezpečena, existujících hrozeb a protiopatření.
    e) Kategorizaci informací v oblasti jejich působnosti z hlediska důvěrnosti a schvalování práv k přístupu k těmto informacím.
    f) Zajištění ustanovení odpovídajících bezpečnostních požadavků a opatření, pokud stávající bezpečnostní opatření nejsou dostatečná.

g) Uplatňování bezpečnostních požadavků v souladu s požadavky bezpečnostních norem.

h) Zajištění takových podmínek pro zaměstnance, a smluvní partnery, aby mohli bez překážek předávat všechny informace týkající se bezpečnosti odpovědným osobám.

i) Vymezení pravomocí a povinností svých podřízených s důrazem na to, aby se nevyskytovala činnost či aktivita, za kterou by nikdo neodpovídal, a aby nedocházelo ke střetu pravomocí.

j) Okamžité hlášení odpovědným osobám o všem, co může mít vliv (změny, poruchy, chyby, incidenty, atd.) na snížení ochrany aktiv, a zejména pak na vznik negativních událostí a bezpečnostních incidentů.

5. Všichni zaměstnanci odpovídají za:

a) Předcházení negativním událostem a bezpečnostním incidentům.

b) Aktivní postup při odhalování a likvidaci následků negativních událostí podle doporučení odpovědné osoby.

c) Oznámení jakéhokoliv porušení tohoto bezpečnostního řádu a navazujících interních řídících dokumentů svému přímému nadřízenému a POB

d) Včasné a úplné předávání informací odpovědné osobě při šetření negativních událostí a dále pak za spolupráci při tomto šetření.

6. Všichni zaměstnanci jsou povinni:

a) Dodržovat bezpečnostní řády Vydavatele a ÚMČK a navazující interní řídící dokumenty.

b) Zajišťovat a prosazovat bezpečnostní řád a interní řídící dokumenty ve smluvních vztazích.

c) Spolupracovat při řešení negativních událostí a bezpečnostních incidentů.

7. Všichni zaměstnanci jsou oprávněni:

a) Vyžadovat výklad svých práv a povinností, které jsou jim uloženy veškerými bezpečnostními dokumentacemi Vydavatele.

b) Vyžadovat od POB pomoc při řešení bezpečnostních problémů.

c) Vyžadovat prošetření bezpečnostních incidentů, problémů a havárií.

8. POB vykonává koordinační a metodickou činnost pro:

a) Objektovou a technickou bezpečnost.

b) Personální bezpečnost.

c) Administrativní bezpečnost.

d) Školení bezpečnosti.

e) Bezpečnost informačních systémů.

f) Bezpečnost sítí.

g) Ochranu interních informací.

h) Agendu ochrany osobních údajů ve smyslu zákona.

i) Kryptografickou ochranu.

j) Výkon certifikační autority.

k) Evidenci, analýzu a řešení negativních událostí.

l) Spolupráci s orgány činnými v trestním řízení při ochraně aktiv ÚMČK na základě zmocnění Vydavatele.

m) Komunikaci s Úřadem pro ochranu osobních údajů.

9. POB je povinen:

a) Zajistit rozpracování tohoto řádu a zásad bezpečnostní politiky do další bezpečnostní řídící dokumentace.

b) Metodicky vést bezpečnostní pracovníky a ostatní zaměstnance.

c) Zajišťovat tok informací tak, aby bylo vedení ÚMČK i Vydavatele včas informováno o všech bezpečnostně významných událostech.

d) Spolupracovat se všemi organizačními složkami Vydavatele při naplňování jejich plánů, cílů a záměrů.

e) Analyzovat, definovat a monitorovat bezpečnostní rizika a krizové situace.

f) Navrhovat a realizovat protiopatření ke zvládání bezpečnostních rizik a krizových situací.

g) Analyzovat bezpečnostní rizika a možné krizové situace spojené s činností ÚMČK, klasifikovat je a zpracovávat opatření k jejich eliminaci či minimalizaci.

h) Koordinovat zpracování plánů pro minimalizaci jednotlivých bezpečnostních rizik či kritických situací.

i) Přijímat preventivní opatření k zamezení nebo minimalizaci rizik a důsledků krizových situací a monitorovat naplnění těchto opatření.

j) Předkládat odborná stanoviska k návrhům havarijních plánů (plánů nepřetržitosti, obnovy funkčnosti atd.).

k) Školit zaměstnance ÚMČK v oblasti bezpečnosti a plánování obnovy funkčnosti ÚMČK při mimořádných událostech.

10. POB je oprávněn:

a) Schvalovat nasazování bezpečnostních systémů, technologií, služeb a procedur.

b) Seznamovat se s výsledky bezpečnostních kontrol.

c) Vyžadovat plnění bezpečnostních opatření.

d) Požadovat v rámci vnitřního vyšetřování negativních událostí ústní i písemná vyjádření od zúčastněných zaměstnanců ÚMČK i Vydavatele.

e) Požadovat spolupráci od všech zaměstnanců Vydavatele.

f) Nahlížet v nezbytném rozsahu do všech potřebných materiálů, dokladů, záznamů a evidencí a v případě potřeby pořizovat jejich kopie.

g) Monitorovat při dodržení právních předpisů a stanovených zásad činnost uživatelů a bezpečnostně významné události v informačních a bezpečnostních systémech ÚMČK a Vydavatele.

h) Vstupovat do všech objektů a na všechna pracoviště ÚMČK a Vydavatele při dodržování interních zásad a pravidel pro pohyb a práci na těchto pracovištích.

i) Udělovat s ohledem na místní podmínky dočasné, popř. trvalé písemné výjimky z platných bezpečnostních předpisů ÚMČK a Vydavatele a jiných vnitřních bezpečnostních řídících dokumentů. Výjimka může být udělena jen v odůvodněných případech. Pokud jsou výjimky uděleny, musí být min. každých 6 měsíců přezkoumáno, zda nepominuly důvody pro jejich udělení a zda se nemění úroveň rizik. Neakceptovatelné zvýšení rizik je důvodem pro neudělení nebo zrušení výjimky.

j) Podávat v odůvodněných případech návrhy na zahájení disciplinárních a kárných řízení.

#### 5.2.6. Personální bezpečnost

1. Vedoucí personálního odboru Vydavatele je odpovědný za prosazování a realizaci personálních bezpečnostních opatření v procesech realizovaných personálním odborem.
2. Při vytváření a změnách charakteristik pracovních pozic je nutné brát v úvahu bezpečnostní aspekty. Jim odpovídající bezpečnostní požadavky musí být zahrnuty do charakteristiky pracovní pozice.
3. Bezpečnostní kritéria pro konkrétní pozice stanoví personální odbor Vydavatele ve spolupráci s POB, ředitelem MČK a přímým nadřízeným pro danou pozici.
4. Splnění bezpečnostních kriterií pro konkrétní pracovní pozici kontroluje bezprostředně nadřízený zaměstnanec.
5. Klíčové pozice musí být identifikovány a ke každé musí vždy existovat kompetentní zástupce. Kriteria výběru klíčových pozic stanoví ředitel ÚMČK.
6. S bezpečnostními požadavky ÚMČK musí být přijímaný zaměstnanec prokazatelně seznámen. Jejich dodržování se musí kontrolovat a vyhodnocovat během pracovního poměru každého zaměstnance.
7. Výběr zaměstnanců musí být mimo jiné založen na jasně stanovených kritériích výběru z hlediska bezpečnostní způsobilosti, důvěryhodnosti a spolehlivosti.
8. Pro získávání, udržování a zvyšování bezpečnostního vědomí je nutné provádět školení bezpečnosti.

#### 5.2.7. Objektová a technická bezpečnost

1. Úroveň objektové bezpečnosti v rámci veškerých objektů, kde je umístěn jakýkoliv prvek ISMČK, stanoví interní řídící dokument.
2. Objekty, v nichž je třeba uplatňovat nástroje prosazující bezpečnost, musí být klasifikovány podle důležitosti.

3. Systémy technické a objektové bezpečnosti musí zajistit aktiva ÚMČK před neoprávněným přístupem, náhodným i úmyslným poškozením a před přírodními riziky.
4. Účinnost technických prostředků musí být pravidelně ověřována.
5. Podmínky vstupu do objektů a prostor ÚMČK a Vydavatele a podmínky jejich opouštění musí být stanoveny interním řídícím dokumentem.
6. POB spolupracuje s vedením Vydavatele při zjišťování rizik (prováděnými preventivními kontrolami pracovišť) a jejich odstraňování. Tato rizika jsou odstraňována opatřeními organizačními nebo technickými.

#### 5.2.8. Bezpečnostní politika informací

1. Hlavním cílem bezpečnostní politiky informací ÚMČK je zajištění trvalého naplňování poslání, dlouhodobých a strategických cílů a plánů ÚMČK, zajištění právní shody s národní i nadnárodní legislativou, relevantní pro činnost ÚMČK a zajištění dostupnosti, integrity a důvěrnosti aktiv ÚMČK, zejména informačních aktiv. Dalšími cíli je zabezpečit správnou a bezpečnou funkci IS, ochranu důvěrnosti, integrity a dostupnosti v celém životním cyklu informačního systému, zabránit neoprávněnému přístupu k IS, fyzickému poškození a vzájemnému negativnímu ovlivnění služeb IS.
2. Bezpečnostní opatření pro ochranu informací musí být implementovány do odpovídajících dokumentů, upravujících vnitřní chod ÚMČK.
3. Vedení Vydavatele i ÚMČK musí podporovat stanovené cíle bezpečnosti informací. Vedení Vydavatele a ÚMČK vyjadřuje touto bezpečnostní politikou informací svoji strategii trvalého zajišťování bezpečnosti informací jako nedílné součásti řídících procesů Vydavatele a MČK.
4. Všichni uživatelé IS musí být vyškoleni ve správné aplikaci bezpečnostních postupů.

### 5.3. Bezpečnostní politika

Stanovuje základní principy a požadavky na bezpečnost ISMČK.

#### 5.3.1. Cíl

Cílem této bezpečnostní politiky je stanovit základní bezpečnostní požadavky na bezpečnost ISMČK v prostředí Vydavatele.

Cílem bezpečnostní politiky Vydavatele pro ISMČK je splnění bezpečnostních požadavků ISMČK a eliminace bezpečnostních rizik, t.j.:

- zajištění důvěrnosti: ochrana informací proti neautorizovanému vyzrazení;
- zajištění integrity: ochrana informací před neautorizovanou nebo náhodnou modifikací a zajištění správnosti a úplnosti těchto údajů a informací;
- zajištění dostupnosti: zabezpečení informací tak, aby byly dostupné vždy, když je to potřebné v souladu s funkcemi, které má ISMČK plnit.

Pro zajištění toho Vydavatel musí:

- chránit veškerá aktiva, která má pod kontrolou. Toto bude dosaženo implementací technických a netechnických (organizačních a personálních) opatření.
- provádět účinnou a efektivní ochranu úměrnou rizikům působícím na aktiva.
- implementovat bezpečnostní politiku informací konzistentně, plánovitě a efektivně.

#### 5.3.2. Působnost

Tato politika je platná pro ISMČK, sítě, aplikace, lokality a uživatele v rámci ISMČK.

#### 5.3.3. Soulad s normami

Bezpečnostní pravidla a postupy pro ISMČK musí být v souladu s platnou legislativou. Jako klíčové je třeba uvažovat zejména následující zákony a normy:

- Obchodní zákoník č. 513/1991 Sb., ve znění pozdějších předpisů - definice obchodního tajemství, označení důvěrných informací, bezpečnostní požadavky ve smlouvách.
- Zákonem č. 262/2006 Sb., zákoník práce ve znění pozdějších předpisů – personální bezpečnost, zaměstnanec jako uživatel, vzdělávání, kontrola, odpovědnost za škodu.
- Zákonem č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů
- Zákonem č. 97/1974 Sb., o archivnictví ve znění pozdějších předpisů
- Zákonem č. 101/2000 Sb., o ochraně osobních údajů ve znění pozdějších předpisů
- CSN ISO/IEC TR 13335-1,2 – Směrnice pro řízení bezpečnosti IT

Východiskem pro zpracování Bezpečnostní politiky ÚMČK v oblasti IT byly především normy ČSN ISO/IEC TR13335-1,2, které popisují základní koncepce pro správu IT, popisují základní role odpovědnosti pracovníků všech úrovní, popisují zacházení s aktivy organizace a hrozbami, které tato aktiva ohrožují. Účelem těchto norem není dát přesný návod na realizaci bezpečnosti IT v organizaci, ale upozornit na některé aspekty bezpečnosti, které není možné při realizaci bezpečnosti pominout. Tento dokument se řídí doporučeními této normy v oblastech, kde to je účelné.

#### 5.3.4. Provozní bezpečnostní procedury

Pro správu ISMČK a sítě musí být vytvořeny bezpečnostní procedury a plány obnovy funkčnosti.

Tyto procedury musí být schváleny dle organizačního řádu vydavatele.

### 5.3.5. Sankce a postihy

Nezodpovědné a nesprávné chování nebo porušení či nedodržení pravidel a předpisů může vést k postihům, či trestnímu stíhání dle platných právních norem ČR a předpisů Vydavatele.

### 5.3.6. Klasifikace informací

Uživatel, který se podílí na vzniku informace, musí zvážit aspekty bezpečnosti informací (jako jsou důvěrnost, integrita, dostupnost a případně i nepopiratelnost a autentičnost). V souvislosti s těmito aspekty je třeba s informacemi vhodně zacházet. Aby se rozlišily požadavky na bezpečnost u jednotlivých informací, zavádí se pro práci s informacemi klasifikace.

Informace se dělí na:

**Veřejné** - mohou být zveřejňovány.

**Neveřejné** - neveřejnými informacemi nazýváme takové informace, jejichž prozrazení, zcizení, nechtěné či úmyslné zveřejnění může omezit nebo znemožnit řádné fungování provozovatele ISMČK či jiného účastníka.

Neveřejné informace dále členíme podle charakteru informace na:

- **důvěrné** – určené pouze pro adresáta;
- **osobní** a citlivé údaje ve smyslu zákona č. 101/2000 Sb.;
- **obchodní tajemství** ve smyslu zákona č. 513/1991 Sb.

### 5.3.7. Zabezpečení ISMČK

Identifikace a autentizace uživatelů

- Všichni uživatelé musí mít přiděleno unikátní uživatelské jméno (identifikátor). Toto uživatelské jméno zajistí, že je možné sledovat činnost jednotlivců v systému. Hesla musí být uložena v takové podobě, aby nikdo včetně správce systému nemohl přečíst uložené heslo. Při distribuci hesel musí být zajištěna jejich důvěrnost.

Autorizace

- Pro přístup k ISMČK musí existovat formální procedury registrace a deregistrace.
- Přístup k datům ISMČK je přidělován na základě definovaných rolí uživatelů v ISMČK.
- Přístup k privilegovaným funkcím uživatele je omezen na pracovníky, kteří mají potřebu takové funkce používat. Přístupová práva uživatele jsou definována příslušnou rolí.
- ISMČK:
  a) řídí přístup uživatelů k datům a funkcím systému na základě definované role uživatele ISMČK

b) zajišťuje ochranu před neautorizovanými přístupy jakýmkoli pomocným programovým vybavením

c) neohrožuje bezpečnost jiných systémů

Evidence a analýza událostí

- Aby bylo možné dokončit důkladnou analýzu libovolné podezřelé události, musí být zaznamenáváno dostatečné množství informací. Časy událostí mohou být důležité při vyšetřování libovolného bezpečnostního incidentu. Proto je nutné, aby všechny hodiny v systému pracovaly podle společného standardu a byl zajištěn jednotný čas v celém ISMČK na všech stanicích a serverech.
- Přístup do logů musí být chráněn, aby se zabránilo jakémukoli možnému zneužití či ohrožení.
- Log musí být udržován po definovanou archivační dobu od okamžiku vzniku. Archivační dobu určuje příslušný předpis Vydavatele (Archivační řád).
- Log musí být pravidelně analyzován, aby se zajistilo, že uživatelé provádí pouze procesy, pro jejichž realizaci byli autorizováni.
- Přístup k datovým souborům musí být chráněn tak, aby bylo zabráněno jakémukoli možnému zneužití nebo ohrožení.

Ochrana proti virům a parazitním kódům

- Ochrana ISMČK proti virům a parazitním kódům se řídí platnými předpisy Vydavatele a smluvních subjektů.

Zálohování a archivace

- Zálohování OS a DB se řídí platnými předpisy pro zálohování.
- Doba archivování se řídí archivačním řádem Vydavatele.

### 5.3.8. Síťové propojení – síťová komunikace

Stav sítě je třeba neustále monitorovat, aby byla umožněna včasná detekce neautorizovaného použití, chyby či závady.

Bezpečnostní požadavky a dostupná bezpečnostní opatření pro síťové služby, které poskytují třetí strany, musí být formálně odsouhlaseny a zdokumentovány. Musí být udržována evidence všech zařízení, a jejich připojení do sítě musí být schváleno POB.

Uzly sítě musí být autentizovány. Pro ověření komunikujících entit musí být použita vzájemná autentizace. Síťová zařízení musí být nastavena takovým způsobem, aby bylo zabráněno neautorizovanému přístupu do sítě nebo k ní připojených systémů. V rámci navázaného spojení musí být zajištěna důvěrnost a integrita.

#### 5.3.9. Slabiny a incidenty

Všechny potenciální slabiny musí být vyšetřeny a doloženy POB. Veškeré bezpečnostní incidenty musí být nahlášeny POB a dále musí být vyšetřeny a evidovány.

#### 5.3.10. Penetrační testování

Je vhodné při každém významném rozšíření systému provést externí penetrační test nezávislou firmou.

#### 5.3.11. Odpovědnost za bezpečnost

Tato kapitola bude konkretizovat seznam rolí v ISMČK a jejich stručný popis.

#### 5.3.12. Platnost

Tato Bezpečnostní politika ISMČK bude revidována průběžně dle rozvoje systému MČK a to pod vedením POB. Současně budou revidovány i návazné procedury, bude-li třeba.

#### 5.3.13. Shrnutí

Bezpečnostní politika jednotlivých součástí ISMČK bude zpracována do samostatných dokumentů, kde budou otázky bezpečnosti popsány detailně. Vznikne sada Bezpečnostní dokumentace ISMČK.

#### 5.3.14. Technická pracoviště (serverovny)

Na těchto pracovištích jsou umístěny servery s aplikacemi a databázemi ISMČK a část síťových prvků. Jsou zde tedy elektronické databáze s transakčními daty ISMČK. Z toho důvodu jsou na zabezpečení těchto pracovišť kladeny nejvyšší nároky. Zároveň je toto zabezpečení nutné pro snížení pravděpodobnosti úspěšnosti útoků s cílem vyřadit ISMČK z činnosti, popř. ovlivnit jeho funkčnost.

Bezpečnostní požadavky uvedené v této sekci je nutné v maximální možné míře aplikovat i na síťové komunikační prvky použité při spojení jednotlivých pracovišť a umístěné mimo tato pracoviště. Vzhledem k šifrované komunikaci je možnost zcizení dat minimální a tak bezpečnost zde zajišťuje ochranu zařízení před útoky s cílem vyřadit systém činnosti.

Zabezpečení a režimová opatření pro serverovny, kde jsou umístěny servery ISMČK, se řídí platnými předpisy.

#### 5.3.15. Zabezpečení komunikací

Zabezpečení komunikace proti ztrátě důvěrnosti a zfalšování dat bude v rámci systému zajištěno šifrováním a autentizací na síťové úrovni. Mezi sítěmi smí být povolen pouze komunikační provoz odpovídající jednotlivým aplikacím a správě a režii sítě. Ostatní komunikace bude být zakázána.

- POB schvaluje připojení všech zařízení do sítě ISMČK
- POB stanoví bezpečnostní požadavky a opatření, zajišťující potřebnou síťovou komunikaci s třetími stranami
- Správce sítě ISMČK zajistí, že jsou nasazena stanovená bezpečnostní opatření, do sítě jsou zapojována pouze schválená zařízení, a tato zařízení eviduje
- Správce sítě ISMČK pravidelně kontroluje evidenci zařízení připojených do sítě a její souhlas s reálným stavem sítě
- Správce sítě ISMČK zajistí nastavením VLAN, filtrací komunikace a autentizací uživatelů, že uživatelé mají přístup pouze k síťovým prostředkům odpovídajícím jejich pracovní náplni.
- Správce sítě ISMČK zajistí ochranu důvěrnosti a integrity komunikace
- Správce sítě ISMČK zajistí, že stav sítě a probíhající komunikace jsou nepřetržitě monitorovány
- Správce sítě ISMČK zajistí, že zdroje pokusů o neoprávněný přístup nebo o zahlcení sítě budou v nejkratší možné době po detekci odpojeny

Vlastní princip zabezpečení sítě a síťové komunikace musí být popsán v následných dokumentech, řešící bezpečnost jednotlivých projektů v rámci ISMČK.

#### 5.3.16. Zabezpečení dat na MČK

Veškerá data ISMČK na MČK jsou ukládána v zašifrované podobě a elektronicky podepsané.

#### 5.3.17. Odpovědnosti uživatelů ISMČK

Mezi základní povinnosti každého uživatele ISMČK patří:

- **Hlášení bezpečnostních incidentů** - jakmile uživatel ISMČK zjistí bezpečnostní incident, má povinnost o této skutečnosti informovat svého nadřízeného, který ihned informuje POB.
- **Hlášení bezpečnostních slabin** - uživatel ISMČK musí v případě zpozorování zaznamenat zranitelná místa nebo hrozby a o této skutečnosti informovat svého nadřízeného, který informuje POB.

- **Hlášení chybného fungování programového vybavení** – o chybném fungování programového vybavení musí uživatel ISMČK informovat svého nadřízeného, který informuje příslušného vedoucího projektu.

Uživatel ISMČK nesmí ponechat **bez dozoru** neveřejné informace. Takové informace mohou být v tištěné i elektronické podobě. Tištěné informace, nebo elektronická média musí být uschovány do vhodných bezpečnostních prostor, opatřených zámkem a obtížně přístupných nepovolaným osobám. Informace v počítači, či podobném elektronickém zařízení, musí být také chráněny, proto je uživatel povinen počítač uzavřít (např. použít heslem chráněný spořič obrazovky) nebo se musí odhlásit od pracovní stanice. V době mimo pracovní dobu a v době dlouhodobé nepřítomnosti uživatele musí být zachována zásada tzv. „prázdného stolu a prázdné obrazovky počítače“ – všechny neveřejné informace musejí být vhodně zabezpečeny před nepovolanými osobami a případnými útočníky.

Bez povolení je zakázáno vynášet zařízení (PC, elektronická média a další), na němž je ISMČK provozován. V případě, že bude zařízení, které bylo využíváno pro provozování systému, vyřazeno z provozu a určeno k jiným činnostem nebo k likvidaci, je nezbytné pro tyto účely si opatřit písemné povolení. Takové povolení vydává správce ISMČK, se souhlasem přímého nadřízeného uživatele ISMČK.

V případě, že uživateli ISMČK byl svěřen přenosný počítač, nebo podobné přenosné zařízení a jsou v něm uloženy neveřejné informace, je nezbytné, aby takové zařízení nebylo nikdy ponecháno bez dozoru. Možnost používání přenosného počítače v ISMČK není zakázána, ale jeho používání v produktivním ISMČK se nedoporučuje.

Důvěrné dokumenty a informace, pokud byly označeny k likvidaci a nebudou dále potřeba, je třeba zničit, aby nebyly obnovitelné (skartovat). Skartace musí být provedena v souladu s platným skartačním a archivačním řádem Vydavatele.

Neoprávněné osoby se nesmí volně pohybovat v prostorech, kde je spravován a provozován ISMČK.

Každý počítač s přístupem k ISMČK je vybaven antivirovým systémem, zajišťujícím ochranu před virovým napadením. Uživatelé jsou povinni žádným způsobem nebránit provozu antivirového systému a výpadek jeho funkčnosti hlásit jako bezpečnostní incident.

Přístup k ISMČK je možný pouze po příslušné autorizaci.

- Systém eviduje uživatele, je schopen sdružovat je do skupin a přidělovat jim přístupová práva pro jednotlivé operace v systému
- Uživatelé se hlásí do jednotlivých modulů pomocí přístupového jména a hesla

Heslo představuje základní prvek počítačové bezpečnosti, a proto musí být kladen na jeho výběr velký důraz, jak u administrátorů, tak i u běžných uživatelů ISMČK. Doporučuje se využít pro tvorbu hesel užití speciálních znaků.

Veškeré aktivity v systému uživatel provádí pouze pod vlastním ID (uživatelským jménem) a pod vlastním heslem. Uživatel je zodpovědný za prováděné aktivity na ISMČK. ID a heslo si každý uživatel chrání proti vyzrazení. Je zakázáno sdílení ID a hesla více osobami.

Uživatel si může měnit heslo k systému kdykoliv požaduje. Pokud bude systém automaticky vyžadovat změnu hesla, je uživatel povinen heslo změnit a není povoleno používat stejného hesla.

Mezi základní atributy kvalitního hesla patří skutečnost, že lze heslo těžko uhodnout. Vlastnosti kvalitního hesla jsou vyjádřeny následujícími body:

- heslo musí být snadno zapamatovatelné, aby uživatel nebyl sváděn k jeho zaznamenání;
- heslo se dá snadno a rychle vložit, je obtížné jeho odpozorování druhou osobou;
- je kombinací malých a velkých písmen a obsahuje i číslice;
- dobré heslo se skládá ze šesti až osmi znaků;
- nesmí obsahovat po sobě jdoucí stejné znaky a nesmí obsahovat pouze číselné nebo pouze písmenné skupiny.

Chyby při tvorbě hesel:

Při tvorbě hesel se obyčejně vyskytuje několik zásadních chyb, kterým je nutné se vyvarovat.

Mezi základní chyby při tvorbě hesel patří:

- Používání hesel jako jsou například demo, test, guest, atp.
- Používání oblíbených hesel jako například datum narození, jména rodinných příslušníků, názvy oblíbených věcí. Je nevhodné používat tato jména i pozpátku nebo doplněna jednoduchým číslem.
- Používání jmen postav ze známých filmů nebo slovíčka z počítačových her. Nevhodné je taky používání známých číselných substitucí ve slovech jako y a z, malé L a číslice 1 atp.
- Používání stejného hesla jako je jméno účtu. Z tohoto důvodu je nutné, aby přístupové účty nebyly nikde zveřejňovány.

Zásadní pravidla pro všechny uživatele ISMČK:

- hesla jsou individuální a musí být držena v tajnosti;
- hesla musí být pravidelně měněna, neprodleně v případě podezření prozrazení hesla;
- při ukončení práce nebo i při krátkém přerušení se musí zaměstnanec odhlásit ze systému, popřípadě uzamknout obrazovku spořičem s heslem;

- přidělené prvotní heslo u aplikací je nutno okamžitě změnit a už více ho nepoužívat;
- umožňuje-li aplikace funkci „ukládání hesla“ je nutno tuto funkcionalitu ignorovat a používat místo toho kvalitní, dobře zapamatovatelná hesla;
- hesla nebudou zahrnuta do žádného automatizovaného přihlašovacího procesu, např. uložení do makra nebo funkční klávesy;
- nesmí dojít k opakovanému použití nebo opakování starých hesel po dobu alespoň pěti změn.

Za dodržování výše uvedených zásad jsou odpovědni všichni uživatelé, kteří mají přístup do ISMČK. Jelikož nedodržení těchto pokynů může mít vážné následky, v případě zjištění těchto skutečností budou vůči zodpovědným osobám uplatněny sankční postihy.

Všichni uživatelé ISMČK jsou vázáni mlčenlivostí, a to i po skončení pracovního poměru u provozovatele. Uživatelé nesmí sdělovat neveřejné informace nepovolaným osobám, nesmí takové informace posílat nezabezpečenou formou e-mailu, či jinou nezabezpečenou formou přenosu. Mlčenlivost se vztahuje i na informace o provozně bezpečnostních opatřeních. Uživatelé nesmí kopírovat žádný software, který je používán v rámci ISMČK, na záložní média (např. disketa, páska, CD a další). Software nesmí být přemisťován na jiné zařízení, ani nesmí být prozrazen nepovolaným osobám a stranám bez písemného souhlasu správce ISMČK. Uživatelé nesmí poskytnuté zařízení a prostředky využívat k soukromým účelům.

Uživatelé nesmí provádět změny standardního nastavení ISMČK (hardwaru i softwaru) bez souhlasu správce ISMČK. Správci ISMČK a sítě jsou zodpovědní za bezchybnou instalaci softwaru na všech zařízeních ISMČK.

Všichni uživatelé ISMČK jsou povinni se řídit platnými směrnicemi a dokumentací, související s ISMČK.

Prostředky, zařízení a informace ISMČK (např. software, dokumentace, seznamy, apod.) mohou být použity pouze pro provozování ISMČK a k zajišťování smluvených služeb pro držitele karet.

Uživatelé nesmějí vyzradit nepovolaným osobám bezpečnostní a kontrolní mechanismy používané v ISMČK a rovněž je zakázáno prozrazovat možné slabiny systému.

Bezpečností mechanismy a opatření je možné sdělit pouze na základě písemné smlouvy, kterou schvaluje POB.

#### 5.3.18. Pravidla pro práci s neveřejnými informacemi

- **Důvěrné**

Důvěrnou informací se rozumí informace, která nemá charakter žádné z ostatních neveřejných informací, ale dle rozhodnutí uživatele je důležité ji alespoň dočasně chránit před zveřejněním a přístupem neoprávněných osob. Je určena úzkému, uživatelem přesně definovanému okruhu osob.

- **Obchodní tajemství**

Neveřejnou informací kategorie "OBCHODNÍ TAJEMSTVÍ" (OT) se rozumí veškeré skutečnosti obchodní, výrobní, či technické povahy související se společností, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu, nejsou v příslušných obchodních kruzích běžně dostupné, mají být podle vůle společnosti utajeny a společnost jejich utajení odpovídajícím způsobem zajišťuje.
Zda informace má skutečně charakter OT určuje uživatel, po dohodě s vedoucím pracovníkem.

- **Osobní a citlivé údaje (OÚ)**

V rámci ISMČK jsou zpracovávány osobní údaje. Obsluha kontaktního (prodejního) místa Vydavatele bude mít k dispozici pouze údaje vytištěné na MČK i údaje v aplikaci ISMČK. Manipulace s OÚ se řídí platnými interními předpisy provozovatele ISMČK.

#### 5.3.19. Zásady při práci s neveřejnými informacemi

Cílem je minimalizovat počet osob, které se neveřejnými informacemi seznamují.
S neveřejnými informacemi se může seznamovat pouze oprávněná osoba. Oprávněnou osobou se rozumí fyzická osoba, která je určena k seznámení s určitou kategorií neveřejné informace pro vymezenou oblast pracovní činnosti, resp. k jejímu zpracování.
Určení oprávněné osoby ke styku s neveřejnou informací kategorie Důvěrné a Obchodní tajemství je dáno náplní její pracovní funkce nebo vyplývá ze zákona.
Rozsah určení je determinován funkcí oprávněné osoby a podmíněn odůvodněnou potřebou seznamovat se s neveřejnou informací. Určení je platné po dobu trvání odůvodněné potřeby seznamovat se s neveřejnou informací ve stanoveném rozsahu.
V odůvodněných případech, z rozhodnutí vedoucího zaměstnance, v jehož působnosti ke zpracování neveřejných informací dochází, může být prováděno písemné určení a vyžadován podpis závazku mlčenlivosti i při styku oprávněné osoby s neveřejnými informacemi kategorie obchodní tajemství.

#### 5.3.20. Administrativní opatření při práci s neveřejnými informacemi

Neveřejný dokument musí být zpracován a manipulace s ním prováděna:

- podle zásad, stanovených vlastníkem úlohy v uživatelské dokumentaci úlohy, ve které dochází ke zpracování neveřejných informací;
- podle obecných zásad stanovených v předpisech Vydavatele.

Při zpracování a manipulaci s neveřejnými informacemi musí být dodržena následující opatření:

**a) Označování neveřejného dokumentu**

Neveřejný dokument listinného charakteru (včetně elektronických editovaných souborů) musí být označen na přední (editované) straně prvního listu v pravé horní části a neveřejný dokument nelistinného charakteru na popisném štítku nebo obalu symbolem:

**“DŮVĚRNÉ” nebo**

**“OBCHODNÍ TAJEMSTVÍ”**

Symbol musí být vyznačen zřetelně a čitelně, v českém jazyce, označení v cizím jazyce je možno používat pouze jako pomocné. U neveřejného dokumentu listinného charakteru musí být symbol vyznačen odlišným typem anebo odlišnou barvou písma od vlastního textu.

Pro neveřejné dokumenty listinného charakteru se využívají formuláře a šablony Vydavatele.

**b) Distribuce**

Distribuce neveřejného dokumentu je prováděna na základě rozhodnutí zpracovatele. Musí být prováděna adresně, s jmenovitým vyznačením adresátů v rozdělovníku neveřejného dokumentu, uloženého u zpracovatele. Nejvhodnější forma distribuce neveřejných dokumentů je předání přímo oprávněným osobám proti podpisu. V elektronické podobě je možná distribuce prostřednictvím e-mailu, vždy s přihlédnutím k charakteru dokumentu a případně s využitím zabezpečení, jako např. šifrování.

Další distribuce neveřejného dokumentu může být prováděna jen s vědomím zpracovatele. O zhotovení kopie, opisu či překladu musí být na původním výtisku dokumentu (nebo souboru v elektronické podobě) vždy pořízen záznam: "Dne …..byla zhotovena kopie v počtu ….. výtisků" a uveden rozdělovník, komu byly kopie zaslány (přiděleny), jméno a podpis osoby, která kopii zhotovila.

Pořízené výpisy či poznámky z neveřejného dokumentu musí být posuzovány zvlášť a podle skutečného obsahu musí být označeny odpovídající kategorií neveřejné informace.

**c) Přeprava neveřejného dokumentu**

Neveřejné dokumenty listinného charakteru i nelistinného charakteru (disketa, CD, USB flash disk) se přepravují kurýrem, držitelem poštovní licence jako doporučené zásilky nebo osobně

určeným uživatelem. Z vnějšího obalu zásilky nesmí být možno zjistit, že se jedná o neveřejný dokument. Pověřené osobě se zásilka předává proti podpisu.

Neveřejné dokumenty v elektronické podobě lze předávat e-mailem pouze s využitím šifrovacích prostředků.

Předávání neveřejných dokumentů prostřednictvím faxu je zakázáno.

**d) Ukládání, archivace a likvidace neveřejného dokumentu**

Neveřejný dokument se ukládá po dobu stanovenou zpracovatelem. Po jejím uplynutí je likvidován nebo archivován, pokud je to dáno zvláštním zákonem.

Likvidace neveřejného dokumentu musí být provedena takovým způsobem, aby nebylo možné neveřejnou informaci jakkoli obnovit.

Lhůty pro ukládání neveřejných dokumentů:

- "DŮVĚRNÉ"

Dobu ukládání stanoví zpracovatel. Po uplynutí této doby se dokument likviduje.

- "OBCHODNÍ TAJEMSTVÍ"

Dobu ukládání stanoví zpracovatel, minimálně po dobu trvání OT. Po uplynutí této doby se dokument archivuje nebo likviduje.

#### 5.3.21. Zabezpečení neveřejných informací zpracovávaných v ISMČK

Zabezpečení se řídí platnými bezpečnostními předpisy provozovatele ISMČK.

**Úschovné objekty**

Neveřejné dokumenty listinného charakteru a nosiče elektronických informací se ukládají v trezorech, uzamykatelných skříních, zásuvkách nebo jiných uzamykatelných schránkách, odděleně od veřejných dokumentů.

#### 5.3.22. Organizační, kontrolní a další opatření

**a) Zabezpečení neveřejných informací při jednání více osob (porady, atp.)**

Při jednáních, jejichž obsahem jsou neveřejné informace, týkající se ISMČK, musí být přijata opatření k zamezení jejich úniku. Jedná se zejména o tato opatření:

- sestavit program jednání tak, aby se s takovou neveřejnou informací nemohly seznámit neoprávněné osoby,
- předem stanovit vymezený okruh účastníků podle oprávnění ke styku s takovou neveřejnou informací,
- vybrat vhodnou místnost a přijmout opatření proti pozorování a vstupu neoprávněných osob,

- před zahájením upozornit zúčastněné na skutečnost, že je projednávána neveřejná informace a na její druh,
- při akcích trvajících déle než jeden den zabezpečit účastníkům jednání bezpečné uložení neveřejných dokumentů,
- jmenovitě a písemně určit pořadatele akce, který odpovídá za dodržování bezpečnostních pravidel po celou dobu jednání,
- vést prezenční listinu, která bude součástí zápisu z jednání.

**b) Bezpečnostní vzdělávání**

S novými uživateli ISMČK musí být bezprostředně před zahájením činnosti s neveřejnými informacemi provedeno školení o obecně platných právních předpisech a řídících dokumentech vztahujících se k zabezpečení neveřejných informací.

Prokazatelné seznámení uživatelů s novelizovanými právními předpisy a řídícími dokumenty, které řeší zabezpečení neveřejných informací se provádí na základě rozhodnutí příslušného vedoucího zaměstnance.

#### 5.3.23. Následná dokumentace ISMČK

Následná dokumentace detailně popisuje jednotlivé funkční, provozní, technické, technologické, servisní a bezpečnostní aspekty aplikace v rámci ISMČK. Tato dokumentace musí vycházet z požadavků na funkčnost, bezpečnost, technologickou aplikovatelnost a přijatelnost následné údržby. Pro každou novou aplikaci, implementovanou v rámci ISMČK, musí existovat minimálně tyto následné dokumenty :

- Samostatná analýza rizik pro implementovanou aplikaci a její porovnání s Analýzou rizik ÚMČK a následné vyhodnocení
- Prováděcí projekt aplikace (funkcionalita, HW, SW, identifikace, vazby, …)
- Bezpečnostní projekt aplikace (popis nakládání s osobními údaji, zabezpečení, …)
- Požadavky na servisní a profylaktickou činnost, zálohování
- Provozní směrnice aplikace
- Plán zálohování a obnovy
- Havarijní plán

Mimo tyto dokumenty mohou vzniknout i další specifické dokumenty, vztahující se k implementované aplikaci.

Dále by měly v ÚMČK existovat tyto všeobecné dokumenty, vztahující se k ISMČK jako celku:

- Plán zvládání rizik (postup a redukce zjištěných rizik na minimální úroveň, práce se zbytkovými riziky)
- Plán bezpečnosti ISMČK (plán základních akcí bezpečnosti)
- Plán zachování kontinuity hlavních činností (provozuschopnost bez podpory IS, popř. s velkým omezením podpory IS)
- Mapa všech havarijních plánů ÚMČK (stanovení priorit při obnově ISMČK jako celku)
- Plán testování havarijních plánů (stanovení podmínek a postupů pro testování havarijních plánů)
- Plán bezpečnostní výchovy a školení zaměstnanců
- Plán auditů IS (běžné kontroly, interní a externí audity, penetrační testování)

#### 5.3.24. Požadavky na zpracování následné dokumentace

Následná dokumentace implementované aplikace do ISMČK musí vždy splňovat tyto podmínky:

- Musí odpovídat nadřazeným dokumentům:
  - Analýza rizik ÚMČK
  - Bezpečnostní řád ÚMČK
  - Bezpečnostní politika ÚMČK
- Musí odpovídat předmětu plnění v příslušné smlouvě
- Musí jasně a podrobně definovat vlastnosti aplikace
- Musí jasně a podrobně definovat požadavky na HW, OS, zabezpečení aplikace, komunikačních linek
- Musí jasně a podrobně definovat požadavky na uživatele aplikace s rozdělením na jednotlivé role
- Musí jasně a podrobně definovat požadavky na provádění servisních a profylaktických činností

# 6. Závěr

Cílem této práce bylo na základě určení a identifikace rozdílů mezi běžným informačním systémem a systémem multifunkční karty vytvořit tři základní bezpečnostní dokumenty pro systém multifunkční čipové karty. Jedná se o „Analýzu rizik“, Bezpečnostní politiku a „Bezpečnostní řád“. Jako vzorek běžného informačního systému je brán systém běžné akciové společnosti s obratem několika set milionů korun, existujícím IT oddělením, několika detašovanými pracovišti a implementovaným podnikovým informačním systémem.

Jako vzorek systému multifunkční karty byl brán systém městské multifunkční karty, který umožňuje držiteli takové karty zjednodušeným způsobem čerpat služby a to placené ze strany držitele, tak i hrazené například městem, zpravidla v urbanizovaném prostředí. Jako atribut přiřadíme ještě využívání elektronických peněz na takovéto kartě.

Hlavní zjištěné rozdíly mezi těmito informačními systémy jsou: Míra zpracovávaných osobních údajů vlastních a cizích subjektů, míra outsourcingu služeb, přístup třetích subjektů k informačním systémům multifunkční čipové karty a naposledy dynamický až překotný rozvoj systému multifunkční čipové karty. Na základě takto zjištěných rozdílů byly vytvořeny tři vzorové bezpečnostní dokumenty pro systém multifunkční čipové karty. Závěrečné doporučení zní: V dynamicky se rozvíjejícím informačním systému je nutné volit odlišný model (strukturu) bezpečnostní dokumentace, ta je popsána ve vzorovém dokumentu „Bezpečnostní řád“. Dále je nutno ve vrcholové bezpečnostní dokumentaci stanovit požadavky na dílčí následnou dokumentaci. Tyto požadavky jsou vzorově zpracovány v dokumentu „Bezpečnostní politika“. Oba dokumenty pak vychází z provedené Analýzy rizik, která je prvním vzorovým dokumentem. Pro smluvní zajištění bezpečnosti u třetích subjektů je nutné využít právních služeb a tato povinnost musí být v dokumentaci stanovena.

Cíle diplomové práce bylo dosaženo a zpracovaná dokumentace může posloužit jako vzor pro zpracování konkrétní dokumentace v existujícím informačním systému multifunkční čipové karty.

## 7. Seznam použitých zdrojů


1. **Bednář V.** IT bezpečnost je předražená -Lupa.cz. *Lupa.cz.* [Online] 3. 10 2008. [Citace: 27. 12 2010.] http://www.lupa.cz/clanky/it-bezpecnost-je-predrazena/.

2. **Ludvík M., Štědroň B.** *Teorie bezpečnosti počítačových sítí.* Kralice na Hané : Computer Media, 2008. ISBN 978-80-86686-35-6.

3. **Doucek T., Novák L., Svatá V.,.** *Řízení bezpečnosti informací.* Praha : Professional Publishing, 2008. ISBN 978-80-86946-88-7.

4. *Průzkum stavu informační bezpečnosti v ČR v roce 2003.* **DSM, NBÚ, Ernst& Young.** Praha : autor neznámý, 2003.

5. **Habr J., Vepřek J.** *Systémová analýza a syntéza 2.vydání.* Praha : SNTL, 1986.

6. Informační technologie - směrnice pro řízení bezpečnosti IT. *ČSN ISO/IEC TR 13335 1-4* .

7. **Garfinkel S., Spafford G.** *Bezpečnost v Unixu a Internetu v praxi.* Brno : Computer Press, 1998. ISBN 80-7226-0820.

8. **Látal I.a kolektiv.** *Ochrana dat,informací a počítačových systémů.* Praha : Eurounion, 1996.

9. **Josef, Požár.** *Informační bezpečnost.* Plzeň : Aleš Čeněk, s.r.o. , 2005. ISBN 80-86898-38-5.

10. **Doseděl T.** *21 základních pravidel počítačové bezpečnosti.* Brno : CP Books a.s., 2005. ISBN 80-251-0574-1.

11. **Kozler.** Kompatibilita městských čipových karet. *Bakalářská práce.* Praha : ČZU, PEF, KIT, 2009.

12. **Rodryčová D., Staša P.** *Bezpečnost informací jako podmínka prosperity firmy.* místo neznámé : Grada Publishing, 2000. ISBN 80-7169-144-5.

13. **Doseděl T.** *Počítačová bezpečnost a ochrana dat.* Brno : Computer Press, 2004.

## 7.1. Seznam zkratek:

| Zkratka | Význam |
|---|---|
| ID | identifikační prvek (např. číslo) |
| PIN | osobní identifikační číslo (Personal Identification Number) |
| SAM | Secure Access Module |
| HW | hardware |
| SW | software |
| MČK | multifunkční čipová karta |
| MAD | Mifare Application Directory |
| BlackList | seznam zakázaných - blokovaných karet v systému |
| EP | elektronická peněženka |
| DB | Databáze |
| ISMČK | Informační systém Multifunkční čipové karty |
| OÚ | Osobní údaje |
| MČK | Multifunkční čipová karta |
| Vydavatel | Organizace Vydavatele Multifunkční čipové karty |
| POB | Pověřená osoba pro bezpečnost |
| PP | Prováděcí projekt |
| BPo | Bezpečnostní politika |
| IT | Informační technologie |
| VO | Vedoucí odboru (organizační jednotky) |
| OS | Operační systém |
| ZOOÚ | Zákon na ochranu osobních údajů |
| BOZP | Bezpečnost a ochrana zdraví při práci |
| BP | Bezpečnostní projekt |
| IS | Informační systém |
| KOC | Kartové odbavovací centrum |
| PO | Požární ochrana |
| PT | Platební terminály |
| RS | Rezervační systém |
| SZ | Samoobslužné zóny |

## 7.2. Seznam obrázků:



## 7.3. Seznam tabulek: