Zásady ochrany informací v oblasti informačních technologií

Obsah:

1 Úvod

Dokument definuje zásady a pravidla řízení bezpečnosti informací, které jsou zpracovávány za využití informačních technologií v prostředí Ministerstva práce a sociálních věcí.
Obsah dokumentu se nevztahuje na informační systémy pracující s utajovanými skutečnostmi na základě zákona č. 148/1998 Sb., o ochraně utajovaných skutečností, ve znění pozdějších předpisů. Tato problematika je řešena vyhláškou NBÚ č. 56/1999 Sb., o zajištění bezpečnosti informačních systémů nakládajících s utajovanými skutečnostmi, ve znění pozdějších předpisů.
Níže definovaná pravidla[1] vycházejí z platných zákonů a norem vztahujících se k rozsahu působnosti MPSV, zejména:

- zákon č. 435/2004 Sb., o zaměstnanosti
- zákon č. 54/1956 Sb., o nemocenském pojištění zaměstnanců, ve znění pozdějších předpisů
- zákon č. 65/1965 Sb., zákoník práce, ve znění pozdějších předpisů
- zákon č. 71/1967 Sb., o správním řízení (správní řád), ve znění pozdějších předpisů
- zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů
- zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů
- zákon č. 117/1995 Sb., o státní sociální podpoře, ve znění pozdějších předpisů
- zákon č. 143/1992 Sb., o platu a odměnách za pracovní pohotovost v rozpočtových a v některých dalších organizacích a orgánech, ve znění pozdějších předpisů
- zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů
- zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů, ve znění pozdějších předpisů
- zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů
- zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, ve znění pozdějších předpisů
- zákon č. 589/1992 Sb., o pojistném na sociální zabezpečení a o příspěvku na státní politiku zaměstnanosti, ve znění pozdějších předpisů
- nařízení vlády č. 330/2003 Sb., o platových poměrech zaměstnanců ve veřejných službách a správě, ve znění pozdějších předpisů
- ČSN ISO/IEC TR 13335 – směrnice pro řízení bezpečnosti informačních technologií
- ČSN ISO/IEC 17799 – soubor postupů pro řízení informační bezpečnosti
- a další související předpisy

2 Cíle a rozsah

Hlavním cílem dokumentu je stanovit základní bezpečnostní pravidla, která zajistí přístup k datům poskytovaných dílčími informačními systémy Ministerstva práce a sociálních věcí, a zároveň zajistí patřičnou ochranu poskytovaných a uchovávaných dat s ohledem na zachování jejich důvěryhodnosti. Dílčími informačními systémy se rozumí především informační systémy definované v koncepci informatiky resortu MPSV. I tyto informační systémy však mohou být dále členěny na menší samostatné celky (například úřady práce).

[1] Pokud je v textu uveden mužský ekvivalent (např. uživatel), je tím myšlen samozřejmě i ženský ekvivalent (např. uživatelka).

Tam, kde je vyžadován vyšší stupeň ochrany informací je možné definovat pravidla přísnější. Ta však nesmí být v rozporu se základním dokumentem.
Zásady ochrany informací v oblasti informačních technologií jsou vydávané formou příkazu ministra. Tyto zásady jsou platné pro všechny informační systémy a pro všechny zaměstnance MPSV, detašovaných pracovišť posudkové služby a úřadů práce.

3 Řízení bezpečnosti

3.1 Organizace bezpečnosti

Řízení bezpečnosti v oblasti informačních technologií je rozděleno na čtyři základní úrovně.

- Ministr práce a sociálních věcí
- Ředitel odboru informatiky MPSV
- Bezpečnostní správce informačních technologií
- Bezpečnostní správce dílčího informačního systému

3.1.1 Ministr práce a sociálních věcí

Úkolem ministra v oblasti ochrany informací zpracovávaných informačními technologiemi je vydávat provozní bezpečnostní směrnice formou příkazu ministra. Návrhy bezpečnostních směrnic předkládá ministrovi ředitel odboru informatiky prostřednictvím náměstka ekonomického úseku.

3.1.2 Ředitel odboru informatiky MPSV

Ředitel odboru informatiky (OI) zejména:

- předkládá ministrovi návrhy provozních bezpečnostních směrnic
- jmenuje bezpečnostního správce IT
- jako svůj poradní orgán řídí Fórum bezpečnosti IT ustanovené ministrem práce a sociálních věcí.

Fórum bezpečnosti IT zejména:

- předkládá návrhy na změnu dokumentu Zásady ochrany informací v oblasti IT a provozní bezpečnostní směrnice
- sleduje zavedení bezpečnosti v oblasti informačních technologií a prověřuje účinnost stanovených zásad
- zajišťuje povědomí o bezpečnosti, a problémech spojených s řízením bezpečnosti a ochrany informací mezi zaměstnanci resortu MPSV
- sleduje potřebné zdroje spojené s nasazením, a řízením bezpečnosti IT. Jedná se především o lidské zdroje, potřebné znalosti a finanční zajištění bezpečnosti.

Členy fóra bezpečnosti jsou minimálně

- vedoucí oddělení provozu WAN
- vedoucí oddělení výstavby informačních systémů
- vedoucí oddělení vývoje aplikací a provozu informačního systému
- vedoucí oddělení systému služeb zaměstnanosti
- bezpečnostní správce IT

Fórum bezpečnosti svolává ředitel OI podle potřeb a aktuální situace.

3.1.3 Bezpečnostní správce IT

Bezpečnostní správce je kontaktní osobou pro veškeré bezpečnostní incidenty spojené s provozem IT. Zároveň přijímá podněty na změny v oblasti bezpečnosti a ochrany IT od uživatelů datových sítí a prvků, tvořících IS MPSV, tj. uživatelů WAN/MAN a všech připojených LAN. Ze své činnosti se zodpovídá řediteli odboru informatiky MPSV.

Bezpečnostní správce zejména:

- odpovídá za řízení oblasti bezpečnosti IT
- předkládá hlášení o stavu bezpečnosti IT fóru bezpečnosti
- navrhuje aktualizace dokumentu Zásady ochrany informací v oblasti IT a bezpečnostních směrnic. Aktualizované materiály pak předává fóru bezpečnosti
- dohlíží nad zavedením a dodržováním bezpečnostních směrnic v oblasti informačních technologií
- koordinuje zkoumání a řešení vzniklých bezpečnostních událostí v informačních technologiích.

Při kontrole pracoviště je povinen prokázat se průkazem potvrzující jeho identitu a zmocněním vydaným ředitelem odboru informatiky MPSV.

3.1.4 Bezpečnostní správce dílčího informačního systému

Vytváří bezpečnostní politiku pro dílčí informační systémy, nebo jejich části. Bezpečnostní politika dílčího informačního systému upřesňuje dokument Zásady ochrany informací v oblasti IT na základě potřeb dílčího IS. Dílčí bezpečnostní politika IS však nesmí být v rozporu s dokumentem zásad ani bezpečnostními směrnicemi vydanými příkazem ministra.

Bezpečnostní správce dílčího IS koordinuje svou činnost s bezpečnostním správcem IT a s fórem bezpečnosti IT. Ze své činnosti se zodpovídá vlastníkovi dílčího informačního systému, který jej do této funkce jmenuje. Bezpečnostní správce dílčího IS zejména:

- vytváří bezpečnostní politiku dílčího informačního systému a vydává směrnice bezpečnosti
- předkládá hlášení o stavu bezpečnosti dílčího IS fóru bezpečnosti IT a bezpečnostnímu správci IT
- dohlíží nad nasazením a dodržováním bezpečnostní politiky v dílčím informačním systému
- koordinuje zkoumání a řešení vzniklých bezpečnostních událostí v dílčím informačním systému s bezpečnostním správcem IT
- sleduje systémové záznamy dílčího informačního systému
- je povinen se řídit rozhodnutími bezpečnostního správce IT.

3.2 Popis rolí

3.2.1 Vlastník systému

Vlastník systému je vedoucí / řídící zaměstnanec mimo oblast IT, který vytváří podmínky pro provoz informačního systému a definuje pravidla, za kterých je možno poskytovat informace uchovávané v informačním systému. Systémem se rozumí veškeré technické a programové vybavení tvořící informační systém. Činnosti spojené s nastavením pravidel pro poskytování informací může vlastník systému delegovat na správce informačního systému MPSV.

3.2.2 Vlastník dat, informací

Vlastníkem dat je vedoucí / řídící zaměstnanec organizační jednotky, která je zodpovědná za jejich tvorbu a která by byla nejvíce ovlivněna jejich ztrátou. Vlastník dat je zaměstnanec mimo oblast informačních technologií, který zařazuje data do kategorií a určuje, kdo k datům bude mít přístup, případně komu budou data poskytována. Činnosti spojené s nastavením přístupu k datům může buď částečně, nebo úplně delegovat na správce systému.

3.2.3 Správce informačního systému MPSV

Správce informačního systému MPSV zodpovídá vlastníkovi systému za funkčnost systému jako celku a za funkčnost služeb poskytovaných informačním systémem MPSV ostatním organizacím připojeným k informačnímu systému MPSV. Správce IS MPSV provádí práce spojené s provozem systému a zajišťuje sledování vlastností systému.

3.2.4 Správce systému

Správce systému je vlastníkovi dat zodpovědný za provoz a funkčnost systému. Vytváří pracovní postupy na obnovu systému, zálohování a odstavení systému. Zajišťuje řešení problémů spojených s provozem systému.
Na správce systému může vlastník dat delegovat činnosti spojené se zakládáním uživatelských účtů a nastavováním přístupových práv.

3.2.5 Uživatel (zaměstnanec)

Uživatelem se stává každý, kdo se k informačnímu systému připojí a identifikuje se svým přístupovým účtem. Uživatel je povinen dodržovat bezpečnostní směrnice vydané příkazem ministra a další směrnice a postupy spojené s řízením informačního systému (zejména provozní řád).
Uživatelem se rozumí také zaměstnanci externích firem, kteří na základě smluvních vztahů provádějí činnosti v informačním systému.

3.2.6 Anonymní uživatel

Anonymní uživatel je takový uživatel, který využívá některé informace, případně služby poskytované informačním systémem, ale v systému není jednoznačně identifikován. To znamená, že uživatel nebyl ověřen systémem na základě přístupového účtu a hesla, případně na základě osobního certifikátu.

3.3 Řízení bezpečnostních incidentů

Všichni uživatelé informačního systému mají povinnost v případě zjištění, nebo podezření na výskyt bezpečnostního incidentu tuto skutečnost ohlásit. Bezpečnostním incidentem se může stát skutečnost popsaná v příloze „Seznam možných typů hrozeb“, nebo podezřelé (nestandardní) chování informačního systému, případně jeho části.
Oznámení výskytu bezpečnostního incidentu se provádí elektronicky vyplněním formuláře „Hlášení bezpečnostního incidentu“, který je následně uložen jako příloha požadavku systému Help Desk MPSV, kde v poli oblast požadavku zadáme hodnotu „Bezpečnost“. Vyplněný formulář je také možné odeslat elektronickou poštou na e-mail adresu bezpecnost@mpsv.cz. Má-li dílčí informační systém svého vlastního bezpečnostního správce, musí jej uživatel o výskytu incidentu také informovat. V případě nefunkčnosti systému Help Desk MPSV a elektronické pošty je možné incident ohlásit také telefonicky prostřednictvím Dohledového centra MPSV, přičemž elektronické oznámení bude provedeno dodatečně. Dodatečné oznámení provede uživatel, který bezpečnostní incident zjistil, nebo správce systému.
Uživatel, který bezpečnostní incident nahlásil, je povinen spolupracovat při řešení a zkoumání incidentu s bezpečnostním správcem IT, i s bezpečnostním správcem dílčího IS.
Veškeré bezpečnostní incidenty jsou evidovány v systému Help Desk MPSV. Evidenci provádí bezpečnostní správce IT, který je zároveň zodpovědný za jejich vyhodnocení. Při vyhodnocení bezpečnostních incidentů spolupracuje bezpečnostní správce IT podle potřeby s fórem bezpečnosti IT.

3.4 Správa dokumentu

Všichni uživatelé informačního systému mají možnost vyjádřit se k obsahu bezpečnostních směrnic vydaných příkazem ministra. Své náměty a připomínky uživatel podává písemně vyplněním formuláře „Připomínky k řízení bezpečnosti v oblasti IT“, který následně odešle na e-mail adresu bezpecnost@mpsv.cz. Připomínky uživatele budou nejprve posouzeny bezpečnostním správcem IT a následně diskutovány fórem bezpečnosti IT. O vypořádání rozhodne bezpečnostní správce, případně fórum bezpečnosti.
O výsledku jednání bude uživatel písemně informován bezpečnostním správcem IT, nebo fórem bezpečnosti.

Dokument zásady ochrany informací v oblasti IT bude pravidelně revidován. Podkladem pro revize dokumentu budou připomínky k bezpečnostním provozním směrnicím, technickým postupům, případně vývoj v oblasti IT.
Revize dokumentu musí být provedena minimálně jednou za dva roky.

4 Klasifikace informací

Veškeré informace, které jsou zpracovávány informačními technologiemi, musí být zařazeny do kategorie. Typ zvolené kategorie závisí na charakteru informace. Dělení informací do kategorií provádí vlastník dat (viz kapitola „Vlastník dat, informací“).
V případě, že jsou informačním systémem zpracovávány informace z různých kategorií, musí být systém zařazen do nejvyšší kategorie, která je v systému zpracovávána.

4.1 Kategorie informací

- Osobní údaje
- Chráněné informace
- Informace pro vnitřní potřebu
- Informace určené pro zveřejnění

4.1.1 Osobní údaje

Mezi osobní údaje spadají veškeré informace, které je organizace povinna chránit ve smyslu § 4 zákona č.101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů. Pro potřeby ochrany informací v oblasti informačních technologiích budou do kategorie osobních údajů zařazeny také citlivé údaje. Veškeré osobní údaje budou chráněny stejně, jako kdyby se jednalo o údaje citlivé.
Informace, která nebude zařazena mezi osobní údaje, bude klasifikována jednou z kategorií definovaných v článku 4.1.2 až 4.1.4.

4.1.2 Chráněné informace

Do kategorie chráněné se informace zařazuje v případě, že její vyzrazení, a to i uvnitř organizace, ztráta, chybné použití, neoprávněná modifikace nebo přístup neoprávněné osoby k ní mohou závažně ohrozit či ztížit činnost organizace, mít závažné negativní právní důsledky pro organizaci, například způsobit újmu fyzické nebo právnické osobě, která informaci poskytla, nebo které se informace týká, přičemž se tato osoba může domoci náhrady za tuto újmu.
Pro potřeby ochrany informací v oblasti informačních technologiích budou do kategorie chráněné informace zařazeny také zvláštní skutečnosti definované zákonem č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů, ve znění pozdějších předpisů.

4.1.3 Informace pro vnitřní potřebu

Do kategorie pro vnitřní potřebu se informace zařazuje v případě, že svým obsahem nespadá do kategorie chráněné a do kategorie určené pro zveřejnění. Jedná se zejména o informaci vzniklou při přípravě rozhodnutí, a to do doby, kdy příprava končí rozhodnutím, informace vztahující se výlučně k vnitřním pokynům a další informace, které orgán veřejné správy podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, neposkytne nebo může omezit jejich poskytnutí. Do kategorie pro vnitřní potřebu se informace zařazuje rovněž v případě, že svým obsahem nespadá do kategorie chráněné a zároveň zvláštní zákon neumožňuje její zveřejnění nebo v určitých případech umožňuje odepřít její zpřístupnění (např. informace se týká dosud nezpracovaných nebo nevyhodnocených údajů).

4.1.4 Informace určené pro zveřejnění

Do kategorie určené pro zveřejnění se informace zařazuje v případě, kdy se jedná o informaci, kterou je orgán veřejné správy povinen zveřejnit podle zvláštního zákona, např. zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, nebo o informaci, o jejímž zveřejnění organizace rozhodne (tisková prohlášení, informativní materiály, nabídky pracovních příležitostí apod.).

5 Značení informací

Aby bylo možné zajistit patřičnou ochranu informací, je nutné informace klasifikovat a následně označit. Vzhledem k tomu, že v prostředí IS MPSV je většina informací zařazena do kategorie pro vnitřní potřebu, nebude u této kategorie označení klasifikace vyžadováno (veškeré informace, které nebudou označeny, budou automaticky náležet do kategorie pro vnitřní potřebu).
Informace v tištěné podobě budou označeny vždy na přední straně prvního listu dokumentu. V netištěné podobě bude označení uvedeno na popisném štítku, obálce, obalu a podobně. Rovněž v případě zobrazení informace na obrazovce musí být informace příslušným způsobem označena, nebo musí být zaměstnanci, kterému se informace zobrazila, prokazatelně známo, do které kategorie je informace zařazena.
Pro značení informací budou používány následující slova a zkratky:

- osobní údaje jsou značeny slovy „Osobní údaje“, nebo zkratkou „OSÚ“
- chráněné informace jsou značeny slovy „Chráněné informace“, nebo zkratkou „CH“. V případě zvláštních skutečností je označení provedeno slovy „Zvláštní skutečnosti“, nebo zkratkou „ZS“.
- informace pro vnitřní potřebu jsou značeny slovy „Pro vnitřní potřebu“, nebo zkratkou „VP“
- informace určené pro zveřejnění jsou značeny slovy „Veřejné“, nebo zkratkou „VEŘ“.

5.1 Osobní údaje

Označování informací zařazených do kategorie Osobní údaje se provádí ve tvaru zkratka organizace, pomlčka, označení kategorie, nebo zkratka názvu kategorie, čárka, jméno zaměstnance, který kategorii stanovil, čárka a datum, kdy tak učinil (například: MPSV-OSÚ, Josef Novák, 21-12-2004). Informace zařazené do této kategorie musí být označovány vždy, i při ústním styku, upozorněním na stanovenou kategorii.

5.2 Chráněné informace

Označování informací zařazených do kategorie Chráněné informace se provádí ve tvaru zkratka organizace, pomlčka, označení kategorie, nebo zkratka názvu kategorie, čárka, jméno zaměstnance, který kategorii stanovil, čárka a datum, kdy tak učinil (například: MPSV-CH, Josef Novák, 21-12-2004). Informace zařazené do této kategorie musí být označovány vždy, i při ústním styku, upozorněním na stanovenou kategorii.
Označování zvláštních skutečností bude provedeno v souladu se zákonem č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů, ve znění pozdějších předpisů pouze slovy „Zvláštní skutečnosti“, nebo zkratkou „ZS“.

5.3 Informace pro vnitřní potřebu

Informace, které jsou zařazeny do kategorie pro vnitřní potřebu nemusí být označené. Pokud informace pro vnitřní potřebu bude označena, například při předání informace na jiný úřad veřejné, případně státní správy, bude označení použito ve tvaru zkratka organizace, pomlčka, označení kategorie, nebo zkratka názvu kategorie, čárka, jméno zaměstnance,

který kategorii stanovil, čárka a datum, kdy tak učinil (například: MPSV-VP, Josef Novák, 21-12-2004).

5.4 Informace určené pro zveřejnění

Označování informací zařazených do kategorie informace určené pro zveřejnění se provádí ve tvaru zkratka organizace, pomlčka, označení kategorie, nebo zkratka názvu kategorie, čárka, jméno zaměstnance, který kategorii stanovil, čárka a datum, kdy tak učinil (například: MPSV-VEŘ, Josef Novák, 21-12-2004).
Označení informace nemusí být použito při vlastním zveřejnění informace, kdy je samotným aktem zveřejnění patrné, že se jedná o informaci určenou pro zveřejnění (například zveřejněním informace na internetu, v tisku, a podobně).

6 Pravidla a zásady pro zajištění bezpečnosti

V této kapitole je uveden výčet ochranných opatření, jejichž splnění zajistí základní bezpečnost informačního systému MPSV.

6.1 Fyzická bezpečnost

6.1.1 Technologické místnosti

Technologickými místnostmi se rozumí taková místa, ve kterých jsou umístěny síťové prvky, aplikační a datové servery. Zejména se jedná o sály výpočetní techniky, datové rozvaděče počítačové sítě a síťové prvky, tvořící komunikační systém resortu MPSV, pomocí kterého probíhá výměna datových, hlasových a obrazových informací, jakož i prostory, poskytující primární a záložní energetické zdroje pro prvky IS MPSV, datová úložiště (trezory s datovými nosiči) a rovněž prostory s technickou dokumentací o informačním a komunikačním systému MPSV.

6.1.2 Zabezpečení technologických místností

Prostory musí být zabezpečeny ve spolupráci s vlastníkem objektu takovým způsobem, aby umožňovaly řízení přístupu do technologické místnosti, a aby bylo možné zabránit vstupu neoprávněných osob.
Při zajištění technologických místností je třeba vzít v úvahu možný výskyt zařízení s nepřetržitým provozem, a možnou přítomnost chráněných informací, nebo osobních údajů.

6.1.3 Řízení přístupu do technologických místností

Přístup do technologických místností musí být umožněn pouze jmenovaným oprávněným zaměstnancům. Jmenování provede vlastník dat (zařízení) uchovávaných v technologických místnostech, který zároveň vede seznam oprávněných zaměstnanců. V seznamu je jmenování potvrzeno podpisem oprávněného zaměstnance. Nacházejí-li se v technologických místnostech data (zařízení) více vlastníků, je nutno o jmenování informovat všechny ostatní vlastníky.
Přístup a pobyt v technologických místnostech ostatním osobám je možný jen za doprovodu oprávněného zaměstnance. O takovéto návštěvě je proveden zápis do provozního deníku, včetně popisu činnosti. Zápis provede oprávněný zaměstnanec.

6.1.4 Provozní deník technologické místnosti

Provozní deník je veden ke každé technologické místnosti. Do provozního deníku jsou mimo jiné uskutečňovány zápisy o činnostech prováděných na zařízení umístěných v technologických místnostech.

6.1.5 Vynášení zařízení z technologických místností

Pro vynešení nebo přinesení zařízení z technologické místnosti je nutný souhlas vlastníka, s jehož zařízením je manipulováno. O pohybu zařízení vede vlastník záznamy a informuje ostatní vlastníky zařízení o manipulaci. Záznamy o manipulaci je možné vést také v provozním deníku technologické místnosti.

6.1.6 Ochrana před výpadkem a chybami napájení

Důležité aktivní prvky sítě, aplikační a datové servery musí být zajištěny před výpadkem elektrické energie napojením na náhradní zdroj elektrického proudu. Náhradní zdroj musí mít takovou kapacitu, aby zajistil elektrické napájení na dobu minimálně 10 minut, plus dobu potřebnou k bezpečnému ukončení systému. Seznam důležitých zařízení definuje vlastník systému.

Náhradní zdroj musí být pravidelně kontrolován. Interval mezi kontrolami je stanoven technickou dokumentací zdroje, zpracovanou výrobcem zdroje. Za pravidelné kontroly zdroje je odpovědný vlastník systému.

Veškerá přípojná místa k elektrickému napájení (elektrické zásuvky) nacházející se v technologických místnostech musejí být ochráněna přepěťovými ochranami.

Pro veškerou výpočetní techniku (nacházející se i mimo technologické místnosti) musejí být vybudované samostatné elektrické rozvody, které budou v místnostech ukončeny na zvláštních označených zásuvkách. Rozvody elektrického napájení musejí být ochráněny před přepětím v síti a nesmí být využívány pro jiná elektrická zařízení.

6.1.7 Ochrana proti vysokým teplotám

Jestliže v technologických místnostech dlouhodobě teplota převyšuje 30°C, z jakýchkoli důvodů, je nutno prostory doplnit o klimatizační jednotku takového výkonu, aby bylo možno udržovat teplotu na úrovni 26°C.

6.1.8 Fyzická ochrana nosičů informací

Nosiči informací se rozumí pevné disky, diskety, pásková média, tiskové sestavy, různé typy paměťových médií a další zařízení, na kterých lze přenášet a uchovávat data.

Nosiče informací je nutno chránit před neoprávněným přístupem umístěním v technologických místnostech, bezpečnostních skříních a podobně. Nosiče nesmí být vystavovány vysokým teplotám (skladovací teplota v rozsahu +5 až +50°C), účinkům magnetického toku, povětrnostním vlivům, vlhkosti a podobně.

V případě vyřazení nosiče vlastník dat zajistí neobnovitelné smazání veškerých dat na něm obsažených (například takzvaný Wiping), nebo jeho fyzické znehodnocení.

6.1.9 Ochrana archivačních médií a zabezpečení manipulace s nimi

Archivační média musí být uchovávána v bezpečnostních skříních, které nejsou umístěny ve stejné místnosti jako data, která jsou na médiu uložena.

Pro zvýšení bezpečnosti archivovaných dat doporučujeme média uchovávat fyzicky v jiné budově (například bezpečnostní schránka v bance).

S médii může pracovat jen osoba pověřená archivací dat. Pověření provede vlastník dat, přičemž o pověření bude vytvořen zápis.

6.1.10 Zabezpečení přenosných zařízení

Přenosná zařízení jako notebooky, organizéry, mobilní telefony a podobné, nesmějí být ponechávány volně bez dozoru mimo pracovní místo zaměstnance. Jsou-li v přenosném zařízení uchovávány jiné informace, než informace určené pro zveřejnění (viz kapitola „Klasifikace informací“), musí být pro jejich ochranu použito přídavných ochranných opatření (kryptografické algoritmy).

6.2 Personální bezpečnost

6.2.1 Postup při vzniku pracovního poměru

Všichni zaměstnanci, kteří budou využívat služby informačního systému, musí být seznámeni s provozními bezpečnostními směrnicemi a se všemi dalšími předpisy týkajícími se provozu IS (provozní řád LAN, WAN).
Při nástupu nového zaměstnance požádá jeho přímý nadřízený vlastníka dat o přidělení potřebných přístupových práv zaměstnance k informačnímu systému a k provozovaným aplikacím. Žádost je nutno podat elektronickou, nebo písemnou formou. Vlastník dat vede evidenci podaných žádostí.
Za všechny činnosti prováděné v informačním systému po dobu potřebnou k zapracování nového zaměstnance (zkušební lhůta), nebo zaměstnance převedeného z jiné činnosti, je odpovědný tento zaměstnanec sám.

6.2.2 Postup při ukončení pracovního poměru

Dnem ukončení pracovního poměru musí být zablokovány všechny přístupové účty využívané zaměstnancem při jeho činnosti. Data, která byla zaměstnancem po dobu pracovního poměru pořízena, mohou být převedena na jiného zaměstnance. O převodu dat rozhodne přímý nadřízený zaměstnance, který data pořídil. Ten zároveň požádá vlastníka dat, případně správce systému, je-li na něj tato povinnost vlastníkem delegována, o převod dat.
Zaměstnanec, který ukončil pracovní poměr, nesmí nadále manipulovat s pořízenými daty, ani tato data záměrně ničit. Veškerá data je zároveň zakázáno přepravovat (na médiu, poštou, a podobně) mimo pracovní místo.
Ve výstupním listu zaměstnance, při ukončení jeho pracovního poměru, správce informačního systému potvrdí zablokování veškerých přístupových účtů tohoto zaměstnance k informačnímu systému.
Obdobně je nutné postupovat i při převedení zaměstnance na jinou organizační jednotku v rámci MPSV.

6.2.3 Dlouhodobé přerušení činnosti v informačním systému

V případě dlouhodobého přerušení činnosti, delší než tři měsíce, (například po dobu mateřské dovolené, pracovní cesty, stáže) musí být po dobu přerušení zablokovány, nebo zrušeny veškeré přístupové účty zaměstnance. Zablokování přístupových účtů musí být provedeno nejpozději v den zahájení dlouhodobého přerušení. Data, která byla zaměstnancem po dobu pracovního poměru pořízena, mohou být převedena na jiného zaměstnance. O převodu dat rozhodne přímý nadřízený zaměstnance, který data pořídil. Ten zároveň požádá vlastníka dat, případně správce systému, je-li na něj tato povinnost vlastníkem delegována, o převod dat.
O zahájení dlouhodobého přerušení činnosti informuje personální oddělení správce systému.

6.2.4 Přístupový účet

Pro zajištění osobní odpovědnosti každého uživatele je nutné pro přístup k informačnímu systému využívat jednoznačný přístupový účet. Přístupový účet je standardně tvořen kombinací uživatelského jména a přístupového hesla, nebo certifikátem uloženým na čipové kartě zaměstnance a PIN kódem čipové karty. Sdílení přístupových účtů několika zaměstnanci je zakázáno. Aby bylo zabráněno zneužití přístupového účtu cizí osobou, musí informační systém po zadání uživatelského jména vyžadovat ještě minimálně zadání přístupového hesla. V případě opakovaného zadání chybné kombinace uživatelského jména a přístupového hesla (tři chybné pokusy) musí být účet minimálně na dobu 30 minut uzamčen.
Zaměstnanec při práci s informačním systémem (informačními systémy) může využívat několik různých přístupových účtů, vyžaduje-li to jeho pracovní náplň.

6.2.5 Přístupové heslo

Přístupové heslo uživatel musí uchovávat v tajnosti a nesmí jej sdělovat jiným zaměstnancům, ani cizím osobám. V případě vyzrazení, nebo podezření na vyzrazení přístupového hesla, je povinen zaměstnanec toto heslo neprodleně změnit. Přístupovým heslem se rozumí také PIN k čipové kartě zaměstnance.
Přístupové heslo uživatele musí mít minimálně pět znaků, přičemž nesmí být stejné s uživatelským jménem zaměstnance. Jedná-li se o privilegovaný účet (viz kapitola Přístupové heslo privilegovaného uživatele), musí být minimální délka hesla osm znaků. Využívá-li zaměstnanec čipové karty, musí být minimální délka PIN kódu čtyři znaky.
Zaměstnanec je povinen minimálně každých šest měsíců přístupové heslo měnit, přičemž nové heslo nesmí být stejné jako heslo předchozí. To neplatí pro PIN čipové karty, který je platný stále. Ke změně přístupového hesla musí být zaměstnanec systémem vyzván automaticky, pokud takovéto nastavení systém umožňuje.
V hesle doporučujeme používat kombinaci velkých a malých písmen, spolu s číslicemi. Heslo by se nemělo shodovat se slovy uvedenými ve slovníku. Odolnost hesla proti násilnému odhalení dále zvýšíme používáním znaků jako je +, -, =, /, \, <, >, $, atd.

6.2.6 Zastupování zaměstnance

V případě zastupování zaměstnance jiným zaměstnancem, budou po dobu zastupování přiřazena zastupujícímu zaměstnanci taková přístupová práva, která mu zajistí vykonávání jeho nové činnosti. S přidělením práv musí souhlasit zastupovaný zaměstnanec, ve výjimečných případech (například při náhlém onemocnění) může souhlas poskytnout také přímý nadřízený zaměstnanec. Přiřazení práv provede vlastník dat (viz kapitola „Vlastník dat, informací“), případně správce systému, je-li na něj tato povinnost vlastníkem dat delegována.
Po ukončení zastupování budou přístupová práva zastupujícímu zaměstnanci opět odebrána. O odebrání práv je povinen požádat zastupovaný zaměstnanec po svém návratu do zaměstnání vlastníka dat, případně správce systému.
V žádném případě nesmí zastupující zaměstnanec ke své činnosti využívat přístupového účtu zaměstnance zastupovaného.

6.2.7 Ustanovení o mlčenlivosti

Zaměstnanec, který má přístup, nebo zpracovává osobní údaje, chráněné informace nebo informace pro vnitřní potřebu je povinen o těchto zachovávat mlčenlivost, pokud zvláštní zákon nestanoví jinak. Povinnost mlčenlivosti trvá i po skončení pracovního poměru, nebo příslušných prací.

6.3 Systémová bezpečnost

6.3.1 Neautorizovaný přístup

Všechny informační systémy musí být nastaveny tak, aby umožňovaly vstup do systému minimálně po zadání přístupového účtu zaměstnance a následného přístupového hesla.
Anonymní přístup k systému je možný jen u takových služeb, které jsou k tomuto účelu určeny. Mezi takové služby patří například internetové a intranetové www servery poskytující obecné informace.

6.3.2 Záznamy systémových událostí

Informační systém musí být nastaven tak, aby v systémových událostech byly dostupné minimálně informace o přihlášení a odhlášení uživatele, a informace o neúspěšných pokusech přístupu k informačnímu systému. Záznamy musí být uchovávány minimálně po dobu čtyř týdnů.
Záznamy musí být pravidelně kontrolovány. Maximální interval kontroly záznamů je jeden týden. Kontrolu záznamů provádí bezpečnostní správce dílčího informačního systému.

V případě, že bezpečnostní správce dílčího informačního systému není jmenován, provádí kontrolu správce systému.

6.3.3 Časová synchronizace

Pro potřeby vyhodnocování systémových událostí musí být veškeré systémy a služby časově synchronizovány.
Pro tyto účely je v prostředí IS MPSV provozována služba přesného času (NTP). Čas poskytovaný službou NTP je v síti MPSV časem referenčním.

6.3.4 Přístupová práva

Přístupová práva uživatele informačního systému musí být nastavena vždy na konkrétní část informačního systému, případně na konkrétní datové a aplikační zdroje. V žádném případě ne na celý informační systém.
Přístupová práva k systému jsou přidělována skupině, nikoli konkrétnímu uživateli. Uživatel je následně přidán do skupiny, ze které práva k systému zdědí. Členem skupiny může být také další skupina. Pouze u systémů, které tento způsob neumožňují mohou být přístupová práva přiřazena přímo uživateli.
Přístupová práva veškerých uživatelů musí být pravidelně revidována. Revize bude zaměřena na neplatné přístupové účty, nesprávně nastavená oprávnění a na změny vlastností informačního systému. Revize se bude provádět alespoň dvakrát ročně, přičemž revize privilegovaných přístupových práv (viz kapitola „Přístupové heslo privilegovaného uživatele“) bude častější (jedenkrát za dva měsíce).
Revizi přístupových práv provádí bezpečnostní správce dílčího informačního systému, případně správce systému, je-li na něj tato povinnost vlastníkem dat delegována.

6.3.5 Zálohování systému

Zálohování informačního systému a uchovávaných dat dělíme na dvě části. Zálohy prováděné za účelem obnovení celého informačního systému po jeho úplném zničení a zálohy prováděné za účelem obnovy části informačního systému, případně části dat zničených, nebo poškozených nevhodným zásahem uživatele, třetí osobou, klimatickými vlivy, živelní pohromou, a podobně.
Pro zajištění základního stupně ochrany, musí být prováděny minimálně zálohy umožňující obnovení celého informačního systému. Interval mezi zálohami nesmí být delší než sedm dní.
Zálohy musí být prováděny pravidelně, na základě vypracovaného plánu zálohování. Do plánu zálohování musí být proveden zápis o každé plánované záloze, včetně jejího výsledku. Plán musí být vypracován tak, aby archivační médium se zálohou bylo uchováno minimálně po dobu čtyř týdnů od provedení zálohy. Součástí plánu zálohování musí být také postup zálohování a seznam dat, která jsou zálohována.
Zálohování systému, včetně příslušné evidence provádí osoba, která byla touto činností pověřena vlastníkem zálohovaných dat. O pověření bude vytvořen zápis.
Je-li v informačním systému provozována aplikace sloužící pro více úřadů současně (například centrální zpracování dat), musí být zajištěno její zálohování v reálném čase prostřednictvím dvou, nebo více, na sobě nezávislých zařízeních. Záložní aplikace musí být umístěna v jiném objektu, než aplikace primární.
Manipulace a nakládání s archivačními médii je řízeno kapitolou „Ochrana archivačních médií a zabezpečení manipulace s nimi“.

6.3.6 Ochrana před škodlivým programovým kódem

Zanesení škodlivého programového kódu do systému (viry, červi, trojské koně, atd.) může mít za následek například nechtěné vyzrazení uchovávaných dat, vyzrazení přístupových hesel, omezení dostupnosti informačního systému, nebo dokonce jeho vyřazení z provozu.

Jako základní ochranná opatření před zavedením škodlivého programového kódu budou nasazeny skenery a zavedeny postupy omezující vložení škodlivého programového kódu do systému.
Skenery – jedná se o softwarové vybavení (např. antivirový program), které se pokouší odhalit škodlivý programový kód. Skenery musí být nasazeny minimálně na všech pracovních stanicích, které se připojují do informačního systému. Aby byla zajištěna jejich spolehlivost, musí být minimálně jedenkrát týdně prováděna aktualizace znalostní báze skenerů (antivirové řetězce), ve které jsou uloženy informace o škodlivých programových kódech. Za pravidelnou aktualizaci znalostní báze skenerů je odpovědný příslušný správce systému. Uživatel nesmí při své práci vyřadit ochranné funkce skeneru z činnost.
Vložení škodlivého programového kódu do systému – může být provedeno například z přenosného (výměnného) média, prostřednictvím elektronické pošty, nebo prostřednictvím sítě. Nositelem programového kódu pak může být spustitelný program, aktivní www stránky, datové soubory obsahující makra a jiné. Před započetím práce s přenosným (výměnným) médiem musí být provedena jeho kontrola na přítomnost škodlivého programového kódu.
Pracovní stanice musí být nastavena tak, aby běžný uživatel nemohl provádět instalaci programového vybavení. Je-li nutné provést instalaci nového programového vybavení, musí pracovní stanice vyžadovat zadání přístupového hesla privilegovaného uživatele.
Na pracovní stanici musí být zakázáno automatické spouštění programů nacházejících se na výměnných médiích (například CD-ROM), pokud je toto nastavení možné.
V případě podezření na přítomnost škodlivého programového kódu v pracovní stanici musí být tato okamžitě odpojena od informačního systému. Opětovné připojení může být provedeno až po důkladné kontrole správcem systému.

6.3.7 Směrování zpráv, informací

Veškeré zpracovávané informace a zprávy, které jsou distribuovány v rámci informačního systému, musí být zachovány uvnitř informačního systému MPSV. Vyžaduje-li informační systém, nebo některá z jeho částí, určitou komunikaci s cizími informačními systémy, je ji možno povolit pouze na základě souhlasu správce informačního systému MPSV. Souhlas však vyžaduje předložení příslušné dokumentace požadované komunikace.
Zvláštní pozornost je třeba v tomto ohledu věnovat informacím, které jsou rozesílány prostřednictvím elektronické pošty. Veškeré prvky, na kterých probíhá zpracování elektronické pošty, musí být nastaveny tak, aby nemohlo dojít k automatickému přesměrování zprávy mimo informační systém MPSV. Výjimku tvoří poštovní brány, které odesílají zprávy do sítě internet a na ostatní subjekty veřejné správy.

6.3.8 Osobní údaje a chráněné informace

Jsou-li v rámci informačního systému MPSV, případně mimo tento informační systém, šířeny osobní údaje, nebo chráněné informace, musí být na jejich ochranu použita přídavná ochranná opatření (kryptografické algoritmy).
V případě zasílání dat prostřednictvím elektronické pošty může být jako vhodné ochranné opatření použito šifrování, s využitím certifikátů vydaných certifikační autoritou (například MPSV). U komunikací mezi aplikacemi navzájem, může být použito šifrované komunikace nad IP protokolem (SSL komunikace).

6.3.9 Uzamčení počítače

Přestane-li zaměstnanec na počítači vykonávat činnost, je povinen se od počítače odhlásit, nebo jinak počítač zajistit před neoprávněným přístupem. Vhodnou formou zajištění počítače je uzamčení pracovní plochy počítače. Povinnost uzamknout pracovní plochu počítače má zaměstnanec i tehdy, opustí-li kancelář či místnost, ve které je počítač umístěn, přeruší-li svoji práci na dobu delší než 10 minut, nebo tak hodlá učinit.
Počítač musí být nastaven tak, aby v přihlašovacím dialogu nebylo zobrazeno jméno naposledy použitého přístupového účtu.

6.3.10 Dokumentace systému, aplikace

Informační systém a každá jeho část, včetně aplikací, musí mít vypracovanou dokumentaci. Dokumentace musí obsahovat popis základních vlastností a funkcí, nastavení proměnných, způsob obsluhy, způsob zálohy a obnovy a postup na ověření správné funkce.
V okamžiku změny vlastností systému, nebo aplikace, musí být provedena také aktualizace dokumentace.
Dokumentace, nebo její části, musí být k dispozici pouze zaměstnancům, kteří s popisovanou částí pracují.
Za vypracování dokumentace je odpovědný vlastník systému.

6.4 Komunikační bezpečnost a bezpečnost IS

6.4.1 Ochrana sítě LAN

Lokální počítačová sít tvoří základní část informačního systému. Lokální síť nabízí přístupové body umožňující využívat služeb informačního systému. Mezi přístupové body patří počítačové zásuvky, informační terminály zapojené do lokální sítě, zařízení umožňující bezdrátové spojení, atd. Z toho důvodu je třeba věnovat zvýšenou pozornost rozmístění přístupových bodů, aby nemohlo dojít k jejich zneužití cizí osobou. Přístupové body se nesmí nacházet na volně přístupných místech bez patřičného zabezpečení. O veškerých přístupových bodech musí být vedena evidence a zaznamenáván jejich stav (aktivní / neaktivní). Evidenci přístupových bodů vede správce systému.

6.4.2 Ochrana sítě WAN, MAN

Rozlehlá datová síť slouží k vzájemnému propojení lokálních počítačových sítí. WAN síť informačního systému MPSV musí být postavena jako neveřejná počítačová síť. Připojení další organizace k informačnímu systému MPSV prostřednictvím WAN sítě může být provedeno teprve na základě souhlasu vlastníka informačního systému MPSV. Rozlehlá datová síť WAN musí poskytovat takovou míru bezpečnosti, aby jejím prostřednictvím mohly být přenášeny neutajované skutečnosti spadající do kategorie informace pro vnitřní potřebu a kategorie určené pro zveřejnění (viz kapitola „Klasifikace informací“), a to bez použití dalších ochranných opatření.

6.4.3 Ochrana síťových prvků

Síťovými prvky se rozumí zařízení typu směrovač, rozbočovač, přepínač, most, převodník, případně další zařízení podílející se na přenosu informací.
Veškeré síťové prvky musí být umístěny v technologických místnostech. Není-li to z topologického hlediska sítě možné, musí být zařízení umístěna v datových rozvaděčích, které umožňují jejich uzamčení.

6.4.4 Topologie sítě WAN

Topologie sítě WAN musí být vyřešena tak, aby MPSV mohlo řídit komunikace mezi jednotlivými organizacemi připojenými k rozlehlé datové síti WAN IS MPSV. WAN síť musí také umožňovat řízení komunikací úřadů v rámci jedné organizace navzájem mezi sebou, přičemž nastavení konkrétních pravidel je v pravomoci MPSV.
MPSV musí mít možnost správy a dohledu nad nastavením všech pravidel definujících bezpečnost a komunikační toky, a zároveň musí mít možnost kontroly nad topologií sítě WAN.
Topologie sítě WAN musí být navržena tak, aby bylo možno zajistit její zálohování do úrovně okresních uzlů prostřednictvím různého média a operátora poskytujícího datové služby.

6.4.5 Dostupnost sítě a služeb IS MPSV

MPSV musí mít možnost pro zajištění kvality a spolehlivosti poskytovaných služeb prostřednictvím informačního systému MPSV sledovat dostupnost všech úřadů, které jsou

připojeny k rozlehlé datové síti WAN, a měřit kvalitu jejich připojení. To platí i pro služby, které jsou v rámci informačního systému MPSV provozovány.

6.4.6 Ochrana připojení k externí síti a k veřejné síti internet

Pro potřeby komunikace informačního systému MPSV s externími sítěmi a se sítí internet musí být využíván sdílený přípojný bod, který může být zálohován. Přípojný bod (body) je sdílen všemi dílčími informačními systémy začleněnými do informačního systému MPSV. Další připojení k externí síti, nebo síti internet je zakázáno. To platí i pro veškerá modemová připojení, byť jen dočasného charakteru.
MPSV musí mít možnost vlastními prostředky řídit veškerou komunikaci procházející přípojným bodem, a to oběma směry. MPSV zároveň určuje, které služby a datové zdroje budou pro informační systém MPSV z externí sítě, nebo ze sítě internet dostupné, a které služby a datové zdroje budou informačním systémem MPSV nabízeny externí síti a síti internet.

6.4.7 Připojení externí organizace k IS MPSV

V případě, že je k informačnímu systému MPSV připojena externí organizace, například pro potřeby správy některé části IS, musí být toto připojení řešeno tak, aby bylo možno technickými prostředky MPSV provádět sledování činnosti externí organizace v IS MPSV, řídit míru přístupu externí organizace k IS MPSV, a v případě podezření na bezpečnostní incident provést i její odpojení. Veškeré tyto činnosti musí mít MPSV možnost provést i bez vědomí připojené externí organizace, s následnou oznamovací povinností.
Externí organizace musí pro přístup k informačnímu systému MPSV používat vyhrazená zařízení, která nebudou součástí informačního systému externí organizace.
Souhlas s připojením externí organizace k IS MPSV vydává správce informačního systému MPSV.

6.5 Administrativní a procedurální bezpečnost

6.5.1 Přístupové heslo privilegovaného uživatele

Privilegovaným uživatelem se rozumí takový uživatel, který má přidělena nejvyšší oprávnění v rámci systému, případně v rámci aplikace. Mezi typické privilegované uživatele patří uživatel Administrator, root, system, atd.
Přístupové heslo privilegovaného uživatele k informačnímu systému, nebo aplikaci musí být uloženo v zalepené obálce, která bude uložena v bezpečnostní schránce. Obálka s heslem musí být pravidelně obměňována. Za uložení obálky do bezpečnostní schránky odpovídá vlastník dat, za pravidelné obměňování správce systému.
Bude-li obálka s uživatelským účtem a přístupovým heslem použita, musí být heslo uživatele změněno na jiné. Heslo musí být také změněno, dojde-li k ukončení pracovního poměru zaměstnance, kterému bylo heslo privilegovaného uživatele známo. Totéž platí i při převedení zaměstnance na jinou činnost.

6.5.2 Pracovní postup na odstavení a znovuspuštění informačního systému

Ke každému informačního systému musí být vypracovány plány na odstavení informačního systému z činnosti a na jeho opětovné uvedení do provozu. Plány vypracovává správce systému. Plány musí být vypracovány pro každý informační systém, nebo každou jeho část odděleně. Součástí plánů musí být i uživatelské účty včetně přístupových hesel, které budou mít dostatečná oprávnění pro provedení popsaných činností. Plány budou umístěny v zalepené obálce, a budou umístěny v bezpečnostní schránce. Za uložení obálky a řízení přístupu do bezpečnostní schránky odpovídá vlastník dat.
Bude-li obálka s pracovním postupem použita, musí být hesla všech uživatelů uvedených v pracovním postupu změněna.

Pracovní postupy musí být pravidelně aktualizovány a testovány. Aktualizace, včetně testu musí být provedena minimálně jedenkrát ročně. V případě, že v důsledku změn informačního systému budou nové i postupy na odstavení a znovuspuštění informačního systému, je nutno pracovní postupy aktualizovat okamžitě. Aktualizaci postupu, včetně testu provede správce systému.

6.5.3 Změna informačního systému, aplikace

Požadavek na změnu informačního systému, nebo aplikace, může být vyvolán potřebami nových vlastností, nebo vývojem v oblasti informačních technologií. Každá změna se ale musí řídit přesnými pravidly. Nejprve je nutné definovat čeho se změna bude týkat. Na základě definice pak bude vypracován popis provedené změny. Popis může být zpracován v několika částech, přičemž každá část může obsahovat jinou míru podrobnosti. Součástí popisu musí být také požadavky na bezpečnostní zajištění systému, personální obsazení, požadavky na kvalifikaci, případně požadavky na vyškolení zaměstnanců. Teprve na základě odsouhlasení všech částí popisu vlastníkem systému (viz kapitola „Vlastník systému“) může být požadovaná změna provedena.
Po dokončení prací spojených se změnou, musí být provedena aktualizace dokumentace systému, aplikace, viz kapitola „Dokumentace systému, aplikace“.

6.5.4 Řízení přístupu k informacím

Povolení přístupu k uchovávaným informacím jiným informačním systémům, nebo jiným zaměstnancům, uděluje vždy vlastník uchovávaných informací, a to vždy pouze na základě platného legislativního předpisu (zákona), nebo na základě písemného rozhodnutí oprávněné osoby MPSV. Jsou-li informace předávány mezi různými organizacemi, musí o tom existovat dokumentace, na základě které správce informačního systému MPSV rozhodne o vytvoření potřebného komunikačního kanálu.

6.5.5 Postupy obnovy informačního systému

Proces obnovy informačního systému může být vyvolán na základě částečného, nebo úplného vyřazení informačního systému z činnosti, případně na základě porušení určitých vlastností systému.
Postupy obnovy musí být vypracovány minimálně pro případ úplného vyřazení informačního systému z činnosti. V postupu musí být zohledněn plán zálohování systému a veškeré další zdroje potřebné pro obnovení činnosti (například místo uložení archivačního média, instalační média systému a aplikací, požadavky na HW vybavení, atd.).
Postupy na obnovu informačního systému vytváří správce systému. Postupy musí být pravidelně aktualizovány. Aktualizace musí být provedena minimálně jedenkrát ročně. V případě, že v důsledku změn informačního systému budou nové i postupy, je nutno pracovní postupy aktualizovat okamžitě. Aktualizaci postupu provede správce systému.
Postupy budou umístěny u vlastníka systému.

6.6 Aplikační bezpečnost

6.6.1 Aplikace vytvořená na zakázku

Je-li v informačním systému MPSV provozována aplikace vytvořená na zakázku pro MPSV, musí být smluvně řešena otázka přístupu ke zdrojovým kódům takovéto aplikace s jejím tvůrcem.
Dříve, než začne být aplikace na zakázku vytvářena, musí být tato skutečnost sdělena odboru informatiky MPSV, nebo odboru informatiky příslušného úřadu. Odbor informatiky musí dát k vytvoření nové aplikace na zakázku souhlas.

6.6.2 Identifikace uživatele v aplikaci

Pro aplikace, ve kterých jsou zpracovávány informace určené pro zveřejnění a informace pro vnitřní potřebu, je dostatečnou identifikací uživatele zadání uživatelského jména a uživatelského hesla. Aplikace pracující s chráněnými informacemi a s osobními údaji vyžadují vyšší stupeň ověření uživatele. Vyšším stupněm ověření se rozumí vložení čipové karty uživatele a zadání hesla, nebo ověření uživatele na základě certifikátu vydaného certifikační autoritou MPSV, případně jinou akreditovanou certifikační autoritou v České republice.

6.6.3 Přístupová práva uživatele na úrovni aplikace

Uživateli musí být v rámci aplikace přidělována jen taková práva, která bezprostředně potřebuje k výkonu své práce.
Přístupová práva uživatele informačního systému musí být nastavena vždy na konkrétní část informačního systému, případně na konkrétní datové a aplikační zdroje. V žádném případě ne na celý informační systém.
Přístupová práva jsou přidělována skupině, nikoli konkrétnímu uživateli. Uživatel je následně přidán do skupiny, ze které práva k aplikaci zdědí. Členem skupiny může být také další skupina. Pouze u aplikací, které tento způsob neumožňují mohou být přístupová práva přiřazena přímo uživateli.
Přístupová práva veškerých uživatelů musí být pravidelně revidována. Revize bude zaměřena na neplatné přístupové účty, nesprávně nastavená oprávnění a na změny vlastností aplikace. Revize se bude provádět alespoň dvakrát ročně, přičemž revize privilegovaných přístupových práv (viz kapitola „Přístupové heslo privilegovaného uživatele“) bude častější (jedenkrát za dva měsíce).
Revizi přístupových práv provádí bezpečnostní správce dílčího informačního systému, případně správce systému, je-li na něj tato povinnost vlastníkem dat delegována.

7 Implementace

Implementací pravidel popsaných v zásadách bezpečnosti IT bude dosaženo základní úrovně ochrany systému.

7.1 Technické postupy

Aby mohla být ochranná opatření nasazena a jejich nasazení zároveň zkontrolováno, musí být vytvořeny technické postupy, které popíší podrobným způsobem implementaci ochranných opatření v každém systému. Technické postupy budou vypracovány pro všechny systémy (operační systémy počítačů, aplikační vybavení, systém zajištění technologických místností, atd.), které se v informačním systému MPSV vyskytují. Technické postupy budou vydávány jako samostatné dokumenty, a budou obsahovat popis pouze pro jeden konkrétní systém. Na základě postupu pak bude moci každý správce systému provést příslušná nastavení.
Vzhledem k tomu, že vývoj v oblasti informačních technologií jde neustále kupředu, budou technické postupy aktualizovány jedenkrát ročně. V případě zásadní změny systému, bude aktualizace provedena okamžitě.
Technické postupy budou sloužit primárně pro správce systémů jako doporučení k nastavení systémů.
Technické postupy zpracovává a vydává odbor informatiky MPSV.

7.2 Bezpečnostní školení

Součástí implementace je také zvyšování povědomí o bezpečnosti všech uživatelů informačního systému. Protože ale každý uživatel vykonává jinou činnost a role uživatelů jsou různé, musí být také bezpečnostní školení prováděna s jinou mírou podrobnosti.

Bezpečnostní školení musí být provedeno minimálně u všech nově nastupujících zaměstnanců, nebo zaměstnanců převedených z jiné činnosti, a to minimálně v době trvání doby potřebné na zapracování zaměstnance. U ostatních zaměstnanců by se školení mělo opakovat jedenkrát ročně. Při změně vlastností ovlivňujících bezpečnost IS musí být školení provedeno u všech zaměstnanců.
V příloze „Bezpečnostní školení“ je vzorová osnova školení se zaměřením na běžného uživatele informačního systému.
Bezpečnostní školení u všech nově nastupujících zaměstnanců provádí jejich přímý nadřízený.
Za zajištění bezpečnostních školení je odpovědný přímý nadřízený.

8 Monitorování a audit

Monitorování bezpečnosti informačního systému si klade za cíl ověřit úroveň implementace bezpečnosti a ve spojení s auditem systému také odhalit nedostatky ve stávající implementaci bezpečnosti. Závěrem provedeného auditu systému pak mohou být doporučení na změnu provozních bezpečnostních směrnic, případně dokumentu zásady ochrany informací v oblasti IT.
Zatímco monitorování bezpečnosti je kontinuální proces, audit je prováděn jednorázově, přičemž audit je možné opakovat s různě dlouhými intervaly.
Pro monitorování systému slouží jako podklad provozní bezpečnostní směrnice a technické postupy, ve kterých je přesně definováno, jak lze požadované bezpečnosti v systému dosáhnout.

8.1 Monitorování

8.1.1 Rozsah monitorování

Monitorování systému musí být prováděno všude tam, kde byla, nebo hodlá být implementována bezpečnost informačních technologií. Monitorování bude zaměřeno na sledování vlastností systému, a zároveň se bude zabývat vyhledáváním nenormálních stavů mezi vlastnostmi (zvýšení zatížení komunikační infrastruktury, nadměrné počty vstupů do technologických místností, časté výpadky aplikací, vysoká četnost neúspěšných pokusů o přihlášení k systému, nebo aplikaci, atd.). Do procesu monitorování musí být zahrnuta veškerá ochranná opatření definovaná pro daný systém.

8.1.2 Organizační zajištění a odpovědnosti

Vlastník dat, nebo systému musí odsouhlasit rozsah monitorovaných vlastností, případně může požadovat jejich rozšíření.
Monitorování provádí správce systému, přičemž může spolupracovat s bezpečnostním správcem. Výsledky monitorování správce systému předkládá vlastníkovi dat, nebo systému, a bezpečnostnímu správci.
Vyhodnocení monitorovaných dat provádí bezpečnostní správce dílčího informačního systému, případně správce systému, je-li na něj tato povinnost vlastníkem dat delegována. Při vyhodnocování spolupracuje s vlastníkem dat, nebo systému.

8.1.3 Prostředky pro monitorování

Vyhodnocení monitorovaných vlastností je jedním ze základních bodů v procesu monitorování systému a zároveň vyžaduje nejvíce času. Vyhodnocení lze provádět dvěma způsoby. Pomocí nástrojů, které automaticky v reálném čase, nebo v určitých časových úsecích vyhodnocují nashromážděná data. Druhým způsobem je pak manuální vyhodnocování dat.

Automatický způsob vyhodnocování dat monitoringem se bude využívat především u takových vlastností systému, které je vhodné sledovat nepřetržitě po celou dobu existence systému. Použité prostředky by pak měly být schopné samy provádět vyhodnocení dat a na základě provedené analýzy informovat o možném nebezpečí, nebo automaticky učinit taková ochranná opatření, která omezí vliv zjištěné hrozby. Následuje příklad dat vhodných pro automatické zpracování.

- přihlášení a odhlášení uživatele
- neautorizované pokusy o přihlášení do systému
- záznam události, transakce
- využití nástrojů a zdrojů operačního systému
- záznam rizikových událostí
- pokus o neautorizované využití služby systému
- a další ...

Manuální způsob je vhodný na ty vlastnosti systému, kde automatické prostředky nejeví dostatečnou účinnost, u vlastností, které jsou převážně statického charakteru, nebo v oblasti monitorování obecného povědomí o bezpečnosti.
Mezi manuální způsoby patří také zjišťování obecného povědomí o bezpečnosti, které je prováděno dotazníkovou metodou, v níž uživatelé odpovídají na otázky z oblasti bezpečnosti.

8.1.4 Vlastní monitorování

Kromě pravidelně se opakujícího monitorování vlastností systému správcem systému, může být učiněno také monitorování bezpečnostním správcem, případně jinou pověřenou osobou.

Vlastní monitorování dělíme na kategorie

- pravidelné – běžné sledování vlastností systému. Monitorování provádí většinou správce systému.
- nárazové – slouží především k zjištění stavu bezpečnosti. Nárazové monitorování provádí většinou bezpečnostní správce, ale může být provedeno i správcem systému.
- vynucené okolnostmi – může být vyvoláno například bezpečnostním incidentem, nebo podezřením na výskyt bezpečnostního incidentu. Tento typ monitorování provádí převážně bezpečnostní správce.

8.1.5 Výsledky monitorování

Výsledky monitorování jsou důležitým podkladem pro celý proces budování a udržení bezpečnosti na dostatečné úrovni.
Výsledky monitorování mohou ukázat na slabá místa systému, případně na jejich základě může být vypracována samostatná bezpečnostní politika pro daný systém.

8.2 Audit

Hlavním cílem auditu je ujistit se, že implementace ochranných opatření v systému, včetně jeho monitorování a řízení je na dostatečně vysoké úrovni, a že celková ochrana systému je přiměřená k rizikům, která na systém působí.
Audit může být proveden vlastními zaměstnanci organizace (interní audit), nebo za využití specializovaných firem (externí audit). Zvláštním druhem auditu je penetrační test, ve kterém je simulován pokus o průnik do systému za využití prostředků poskytovaných systémem.

8.2.1 Interní audit

Zaměstnanec, který interní audit systému provádí, musí být oddělen od každodenních činností spojených s provozem systému. Jedině tak lze docílit nezávislosti a zvýšit možnost

odhalení slabin ve stávající implementaci bezpečnosti. Auditor se ve své činnosti zaměřuje především na následující oblasti

- audit míry implementace bezpečnosti
- revize provozních bezpečnostních směrnic a technických postupů
- audit vývoje systému a změn
- audit operačního systému
- audit aplikačního vybavení
- audit bezpečnosti síťového prostředí a přístupu k systému
- a další ochranná opatření.

8.2.2 Externí audit

Externí audit systému se od interního auditu liší především tím, že je prováděn cizí firmou, která nemá žádné vazby na provoz informačního systému. Externí audit je prováděn za spolupráce správce systému a vlastníka.
Hlavním cílem externího auditu je odhalit nedostatky v bezpečnosti IT, a pokusit se nalézt takové systémy, u kterých je stávající implementace ochranných opatření nedostatečná a pro které by bylo vhodnější vypracovat samostatnou bezpečnostní politiku.

8.2.3 Penetrační test

Prostřednictvím penetračního testu je veden útok na konkrétní cíl, se snahou o úspěšné proniknutí, ovládnutí cíle. Penetrační test může být prováděn interními zaměstnanci, nebo externími zaměstnanci.
O provedení penetračního testu musí být informován vlastník systému (dat), bezpečnostní správce IT a bezpečnostní správce dílčího IS. Samotný test může být ale proveden bez vědomí správce systému.

9 Seznam zkratek

ČSSZ	Česká správa sociálního zabezpečení
SÚIP	Státní úřad inspekce práce
HW	Hardware (technické vybavení, jako jsou počítače, směrovače, přepínače, monitory atd.)
IP	Internet Protocol – síťový protokol
IS	Informační systém
IT	Informační technologie
LAN	Lokální počítačová síť
MAN	Metropolitní počítačová síť (počítačová síť v rámci jednoho města)
MPSV	Ministerstvo práce a sociálních věcí
NTP	Network Time Protocol – distribuce času
OI	Odbor informatiky
PIN	Osobní přístupový kód k čipové kartě
SSL	Secure Sockets Layer - metoda šifrování IP komunikace
VÚBP	Výzkumný ústav bezpečnosti práce
VÚPSV	Výzkumný ústav práce a sociálních věcí
WAN	Rozsáhlá počítačová síť
www	World Wide Web – servery sloužící ke zveřejňování informací

Přílohy

Příloha A – Připomínky k řízení bezpečnosti v oblasti IT

Připomínky k řízení bezpečnosti v oblasti informačních technologií

bezpecnost@mpsv.cz

telefon: 221 922 433 , fax: 221 921 284

Kontaktní údaje

Úřad :

Jméno :

Telefon :

e-mail :

Označení příkazu ministra:

Datum vznesení připomínky:

Číslo kapitoly, případně odstavec, který je připomínkován:

Návrh nového textu: (uveďte navrhovaný text, nebo odkaz na přílohu se změnami)

Příloha B – Hlášení bezpečnostního incidentu

Hlášení bezpečnostního incidentu

bezpecnost@mpsv.cz

telefon: 221 922 433 , fax: 221 921 284

Místo výskytu incidentu Úřad: Adresa:	**Incident nahlásil** Jméno: Telefon: e-mail:
Datum výskytu:	**Čas výskytu:**

Typ bezpečnostního incidentu (viz příloha Seznam možných typů hrozeb, případně i jiný typ)

Způsob vzniku incidentu: úmyslný ☐ náhodný ☐ přírodního charakteru ☐

Popis incidentu (míra poškození, nebo narušení informačního systému, jaká data byla poškozena, případně zcizena, jak dlouho nebyl IS dostupný, kdo podle vás incident způsobil, atd.)

Příloha C – Seznam možných typů hrozeb

V tabulce je uveden seznam různých hrozeb, které se mohou vyskytnout v informačním systému MPSV. U každé hrozby je uveden také možný způsob výskytu hrozby.

- Úmyslná – hrozba, která může nastat úmyslným jednáním za účelem poškodit IS
- Náhodná – hrozba, která může nastat náhodným jednáním lidské aktivity, a která může způsobit náhodné poškození IS
- Přírodní – hrozba, které nemá souvislost s lidským jednáním, a je způsobena vlivy přírody, nebo okolního prostředí

Hrozba	Úmyslná	Náhodná	Přírodní
Analýza provozu (sledování, monitorování, audit)	x		
Elektromagnetická radiace	x	x	x
Elektrostatický náboj			x
Extrémní teplota a vlhkost	x	x	x
Chyba programového vybavení	x	x	
Chybné směrování zpráv, dat	x	x	
Chyba správce	x	x	
Chyba uživatele	x	x	
Krádež	x		
Nedostatek zaměstnanců	x	x	
Nedostupnost služeb sítě, aplikací	x	x	x
Nelegální používání softwaru	x	x	
Neoprávněné použití paměťového média	x		
Nesprávné použití zdrojů, zařízení	x	x	
Neoprávněný přístup k datům, síti – zevnitř	x		
Neoprávněný přístup k datům, síti – zvenku	x		
Neoprávněný vstup do technologické místnosti	x		
Odposlech	x	x	
Poškození paměťového média	x	x	x
Použití síťového vybavení neautorizovaným způsobem	x		
Použití softwaru neautorizovaným způsobem	x	x	
Použití softwaru neautorizovaným uživatelem	x	x	
Použití zbraní	x	x	
Požár	x	x	
Předstírání identity uživatele	x		
Přetížení sítě LAN, WAN	x	x	
Živelní pohromy (úder blesku, povodeň, prach, silný vítr, zemětřesení)	x	x	x
Selhání dodávky energie		x	x
Selhání hardwaru		x	
Selhání klimatizace	x	x	
Selhání sítě LAN	x	x	
Selhání sítě WAN	x	x	
Selhání softwaru	x	x	
Škodlivý software (například vir)	x		
Technické selhání síťových komponent		x	
Úmyslné poškození (HW, SW, budovy, vybavení)	x		
Vymazání, ztráta dat	x	x	
Výpadek elektrického proudu	x	x	x
Vyzrazení přístupového hesla	x	x	
Manipulace s daty, zveřejnění citlivých údajů	x		
Jiný typ hrozby	x	x	x

Příloha D – Bezpečnostní školení

V příloze je uveden příklad osnovy bezpečnostního školení určeného pro uživatele informačního systému.
Hlavním cílem školení je běžného uživatele informačního systému seznámit s provozními bezpečnostními směrnicemi, zvýšit jeho povědomí o bezpečnosti, a zdůraznit roli uživatele v celém systému.

Co je to bezpečnost
- Obecný popis bezpečnosti v informačních systémech (prevence narušení systému, zajištění dostupnosti a důvěryhodnosti, práva a povinnosti uživatelů informačního systému)
- Popis informačního systému MPSV
- Zavedení bezpečnosti do informačního systému
- Typy bezpečnostní politiky
- Na které systémy se řízení bezpečnosti vztahuje

Fyzická bezpečnost
- Budov
- Kanceláří, technologických místností
- Zařízení a vybavení
- Ochrana nosičů informací

Personální bezpečnost
- Zacházení s přístupovým účtem a heslem
- Zastupování zaměstnanců

Systémová bezpečnost
- Zálohování systému a dat
- Ochrana před škodlivým programovým kódem
- Směrování zpráv
- Ochrana pracovní stanice uživatele
- Práce s výměnnými médii

Komunikační bezpečnost
- Topologie sítě LAN, WAN
- Síťová zařízení (směrovače, rozbočovače, přepínače, firewally)
- Připojení k externím sítím a síti Internet

Administrativní bezpečnost
- Kategorizace informací
- Značení informací

Řízení bezpečnosti
- Popis organizace bezpečnosti
- Popis rolí uživatelů
- Řešení bezpečnostních incidentů
- Aktualizace technických postupů a bezpečnostních směrnic
- Životní cyklus bezpečnosti v informačním systému
- Kontroly bezpečnosti, audit systému

Hrozby a zranitelnosti systému