



# VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

**FAKULTA PODNIKATELSKÁ**  
FACULTY OF BUSINESS AND MANAGEMENT

**ÚSTAV INFORMATIKY**  
INSTITUTE OF INFORMATICS

**NÁVRH MANAGEMENTU BEZPEČNOSTI  
INFORMACÍ V MALÉM ÚČETNÍM PODNIKU**  
PROPOSAL INFORMATION SECURITY MANAGEMENT IN SMALL  
ACCOUNTING ENTERPRISE

**DIPLOMOVÁ PRÁCE**  
MASTER'S THESIS

**AUTOR PRÁCE**  
AUTHOR

Bc. Josef Krčmář

**VEDOUCÍ PRÁCE**  
SUPERVISOR

Ing. Viktor Ondrák, Ph.D.

BRNO 2016

# ZADÁNÍ DIPLOMOVÉ PRÁCE

**Krčmář Josef, Bc.**

---

Informační management (6209T015)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

**Návrh managementu bezpečnosti informací v malém účetním podniku**

v anglickém jazyce:

**Proposal Information Security Management in Small Accounting Enterprise**

Pokyny pro vypracování:

Úvod  
Cíle práce, metody a postupy zpracování  
Teoretická východiska práce  
Analýza současného stavu  
Vlastní návrhy řešení  
Závěr  
Seznam použité literatury  
Přílohy

Seznam odborné literatury:

ČSN ISO/IEC 27001:2006 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky. Český normalizační institut, 2006. ČSN ISO/IEC 27002:2005 Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací. Český normalizační institut, 2005.

DOBDA, L. Ochrana dat v informačních systémech. Praha: Grada Publishing, 1998. ISBN 80-716-9479-7.

DOUCEK, P., L. NOVÁK a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.

POŽÁR, J. Základy teorie informační bezpečnosti. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8.

POŽÁR, J. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

Vedoucí diplomové práce: Ing. Viktor Ondrák, Ph.D.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2015/2016.

L.S.

---

doc. RNDr. Bedřich Půža, CSc.  
Ředitel ústavu

---

doc. Ing. et Ing. Stanislav Škapa, Ph.D.  
Děkan fakulty

V Brně, dne 29.2.2016

## **Abstrakt**

Tato diplomová práce navrhuje implementaci systému řízení bezpečnosti informací do reálného podniku zpracovávajícího účetnictví. V první části jsou popsána teoretická východiska. Na jejímž základě, bude provedena analýza společnosti a vytvořen návrh opatření, který bude zvyšovat bezpečnost informací ve vybraném podniku.

## **Abstract**

This diploma thesis proposes the implementation of information security management system in a business processing accounting. The first part describes the theoretical background. On the basis, will analyze the company and created the draft measures that will increase the security of information in a selected company.

## **Klíčová slova**

ISMS, PDCA cyklus, ČSN ISO/IEC 27 001, ČSN ISO/IEC 27002, Analýza rizik, Analýza aktiv

## **Keywords**

ISMS, PDCA cycle, ISO/IEC 27 001, ISO/IEC 27 002, Risk analysis, Analysis of assets

### **Bibliografická citace**

KRČMÁŘ, J. Návrh managementu bezpečnosti informací v malém účetním podniku. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2016. 86 s. Vedoucí diplomové práce Ing. Viktor Ondrák, Ph.D..

### **Čestné prohlášení**

Prohlašuji, že předložena diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 sv., o právu autorském a o právech souvisejících s právem autorským.)

V Brně dne

.....

## **Poděkování**

Touto cestou bych rád poděkoval vedoucímu diplomové práce Ing. Viktoru Ondrákovi, PhD. a Ing. Petru Sedlákovi za cenné rady a připomínky. Dále svým rodičům za veškerou podporu během mého studia.

# Obsah

ÚVOD .....	9
CÍL PRÁCE.....	10
1 TEORETICKÁ VÝCHODISKA .....	11
1.1 Základní pojmy.....	11
1.2 Systém řízení bezpečnosti informací .....	13
1.2.1 Model PDCA.....	13
1.2.2 Ustanovení ISMS .....	15
1.2.3 Zavádění a provoz ISMS .....	16
1.2.4 Monitorování ISMS.....	19
1.2.5 Údržba a zlepšování ISMS .....	19
1.3 Normy řady ISO/IEC 27 00x.....	19
1.3.1 Norma ISO/IEC 27000.....	21
1.3.2 Norma ISO/IEC 27001 .....	21
1.3.3 Norma ISO/IEC 27002.....	21
1.3.4 Norma ISO/IEC 27003.....	22
1.3.5 Norma ISO/IEC 27004.....	22
1.3.6 Norma ISO/IEC 27005 .....	22
1.3.7 Norma ISO/IEC 27006.....	23
1.4 Zákony týkající se bezpečnosti informací v ČR.....	23
1.4.1 Zákon o elektronickém podpisu .....	23
1.4.2 Zákon o archivnictví a spisové službě.....	23
1.4.3 Zákon o ochraně osobních údajů.....	24
1.4.4 Zákon o kybernetické bezpečnosti .....	24
1.5 Analýza aktiv .....	27
1.5.1 Hodnocení aktiv .....	27
1.6 Analýza rizik.....	28
1.6.1 Metodiky analýzy rizik.....	29
1.6.2 Řízení rizik .....	32

2	ANALÝZA SOUČASNÉHO STAVU .....	33
2.1	Informace o podniku.....	33
2.2	Bezpečnost ve firmě .....	33
2.2.1	Fyzická bezpečnost v podniku .....	33
2.2.2	IS/ICT v podniku.....	33
2.2.3	Bezpečnostní politika ve firmě.....	35
2.3	Identifikace aktiv .....	35
2.3.1	Klasifikace aktiv.....	35
2.3.2	Ohodnocení aktiv .....	36
2.4	Identifikace hrozeb .....	37
2.4.1	Klasifikace rizik .....	40
2.4.2	Matice rizik .....	40
2.5	Shrnutí analýzy .....	41
3	NÁVRH ŘEŠENÍ.....	42
3.1	Zavedení ISMS .....	42
3.1.1	Rozsah zavedení ISMS.....	42
3.1.2	Soubor opatření .....	42
3.2	Popis jednotlivých opatření .....	46
3.2.1	Politiky bezpečnosti informací (A.5) .....	46
3.2.2	Organizace bezpečnosti informací (A.6).....	47
3.2.3	Bezpečnost lidských zdrojů (A.7) .....	51
3.2.4	Řízení aktiv (A.8).....	53
3.2.5	Řízení přístupu (A.9).....	58
3.2.6	Kryptografie (A.10).....	61
3.2.7	Fyzická bezpečnost a bezpečnost prostředí (A.11) .....	62
3.2.8	Bezpečnost provozu (A.12).....	66
3.2.9	Bezpečnost komunikací (A.13) .....	69
3.2.10	Vztahy s dodavateli (15) .....	71
3.2.11	Řízení incidentů bezpečnosti informací (A.16).....	71

3.2.12	Soulad s požadavky (A.18) .....	74
3.3	Postup zavedení změn .....	76
3.3.1	Časový plán implementace opatření .....	77
3.4	Ekonomické zhodnocení.....	77
ZÁVĚR.....		80
SEZNAM POUŽITÉ LITERATURY .....		82
SEZNAM OBRÁZKŮ .....		84
SEZNAM TABULEK .....		85
SEZNAM PŘÍLOH .....		86

## ÚVOD

V dnešní době, kdy se snažíme propojit téměř vše prostřednictvím internetu nebo jiných komunikačních kanálů, se informační bezpečnost stala velmi aktuálním tématem. Organizace jsou si vědomy, že informace jako know-how nebo patenty ale i různá data jsou nejcennějším majetkem organizace, ale už zapomínají nebo podceňují jejich ochranu. Mnoho organizací pracuje s digitálním obsahem z důvodů snadnější manipulace, vyhledávání různých informací a jiné úkony. Tím využívají informační technologie, se kterými kromě výhod přichází i hrozby, které jsou potřeba zabezpečit různými opatřeními, aby práce s informačními technologiemi byla co nejbezpečnější.

V organizacích působí mnoho rizik, mezi které patří i zaměstnanci organizace protože mají přístup k důvěrným informacím. Je vhodné, aby i zaměstnanci procházeli různými školeními ohledně bezpečnosti informací z důvodu předejití různých ztrát organizace zničením, poškozením, odcizením důvěrných dat organizace. Zaměstnanci by měli přístup pouze k těm údajům, se kterými musí při výkonu práce manipulovat a znát své odpovědnosti ve funkci, kterou zastává.

Pro malé organizace může být zavádění informační bezpečnosti, příliš nákladné a proto se jí nevěnují na dostačující úrovni. Na základě norem řady ISO/IEC 27 000 je možné dosáhnout na dostačující úroveň zabezpečení informací v organizaci s akceptovatelnými náklady na její implementaci. Zavedený systém bezpečnosti informací si může nechat organizace i certifikovat a vytvořit výhodu před konkurenty.

## **CÍL PRÁCE**

Cílem této práce je vytvořit návrh systému řízení bezpečnosti informací v malé organizaci, která zpracovává účetnictví, podle řady norem ČSN ISO/IEC 27000. Na základě těchto norem je možné získat certifikát potvrzující bezpečnost informací v daném podniku. Jelikož firma nemá v plánu získat tento certifikát, budou tyto normy použity jako doporučení ve snaze zvýšit bezpečnost informací v dané společnosti.

V této práci budou uvedena teoretická východiska, na základě které bude provedena analýza organizace. V teoretické části budou uvedeny normy a zákony týkající se bezpečnosti informací. Následně bude provedena analýza organizace, kde bude zpracována analýza aktiv a analýza rizik. V poslední části budou navržena příslušná bezpečnostní opatření, která budou snižovat analyzovaná rizika organizace. Součástí návrhu bude i zpracování ekonomického a časového plánu na zavedení systému řízení bezpečnosti informací v této účetní organizaci.

# 1 TEORETICKÁ VÝCHODISKA

## 1.1 Základní pojmy

**Data** – vhodným způsobem vyjádřená zpráva, která je srozumitelná pro příjemce této zprávy a přizpůsobená pro další zpracování [1].

**Informace** – Význam, který přiřazujeme datům, údajům a z nich vytvořeným vyšším celkům [1].

**Informační systém (IS)** – Informační systém je možné pochopit jako systém vzájemně propojených informací a procesů, které s těmito informacemi pracují [2].

**Informační a komunikační technologie (ICT)** – Pod tímto termínem se ukrývá veškerá technika zabývající se zpracováním a přenosem informací, které jsou potřeba pro komunikaci [2].

**Dostupnost** – Zajištění přístupnosti k informaci oprávněnému uživateli v daný okamžik [2].

**Důvěrnost** – Zajištění, že daná informace není dostupná nebo není odhalena neautorizovaným uživatelům nebo procesům [1].

**Integrita** – Zajištění správnosti a úplnosti informací [2].

**Bezpečnost informací** – jedná se o ochranu důvěrnosti, dostupnosti a integrity informací. Kromě těchto tří vlastností může obsahovat ještě autenticitu, odpovědnost, nepopiratelnost a spolehlivost [1].

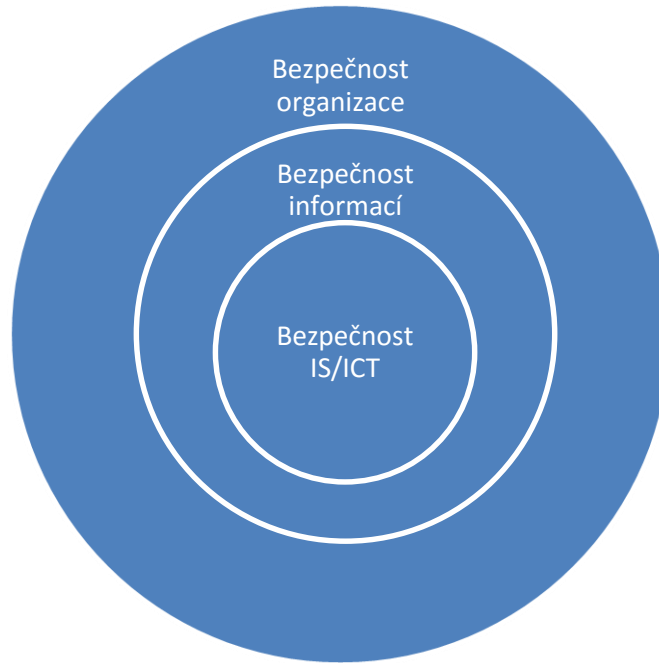
Bezpečnost informací je vzájemným vztahem s bezpečností organizace a bezpečností IS/ICT. Jejich vztah je zobrazen na obrázku č. 1 [2].

Bezpečnost organizace je nejvyšší kategorií bezpečnosti v organizaci. Zahrnuje bezpečnost objektů a majetku organizace jako je ostraha přístupů do organizace nebo objektu pomocí strážní služby [1].

Bezpečnost informací zahrnuje zásady bezpečné práce s informacemi, ať už se to týká informací v digitální nebo nedigitální formě. To obsahuje způsoby zpracování dat, jejich

ukládání, skartace materiálů, zásady transportu dat na jiná místa i zásady vystupování pracovníků v médiích [1].

Bezpečnost IS/ICT ochraňuje jen ty aktiva, která se týkají informačního systému firmy, který je podporován informačními a komunikačními technologiemi [1].



**Obrázek 1 - Vzájemné vztahy bezpečnosti informací v organizaci (Zdroj: [1])**

**Aktivum** – Jedná se o veškerý hmotný a nehmotný majetek ve firmě [2].

**Zranitelnost** - Je slabé místo aktiva nebo opatření, které může vést k neautorizovanému přístupu ke zdrojům systému [1].

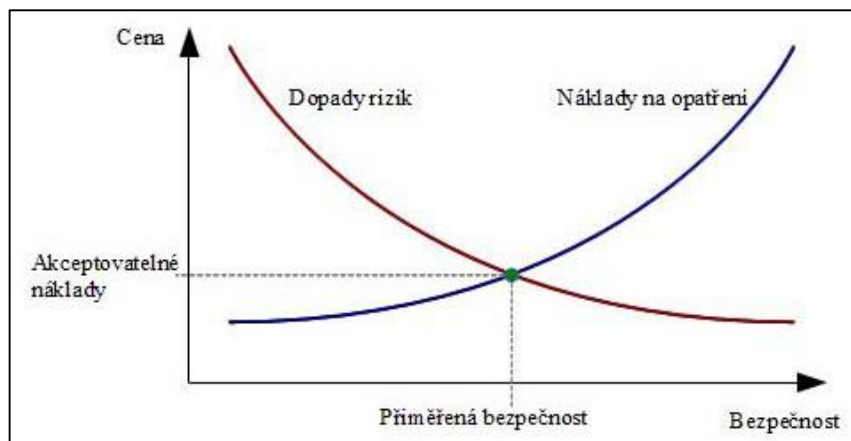
**Hrozba** – potenciální příčina nechtěného incidentu, jehož výsledkem může být událost ohrožující bezpečnost systému nebo organizace. Hrozba je zneužití zranitelnosti [1].

**Opatření** – je postup, který sníží sílu hrozby nebo úplně zabráni v jejím účinku na informační systém [1].

**Riziko** – Společné působení hrozeb působících na aktivum a zranitelnosti daného aktiva [1].

**Dopad** – je vznik škody v důsledku působení hrozby [2].

**Přiměřená bezpečnost** – Úsilí a investice vynaložené na bezpečnost daných aktiv v podniku musí být shodná s hodnotou podnikových aktiv a míře pravděpodobných bezpečnostních rizik. Přiměřenou bezpečnost určuje vedení podniku po ocenění podnikových aktiv, aby bylo možné stanovit výši nákladů na bezpečnost podnikových aktiv. Na obrázku 2 je znázorněn graf určující přiměřenou bezpečnost za akceptovatelné náklady [1][2].



Obrázek 2 - Přiměřená bezpečnost za akceptovatelné náklady (upraveno dle [2])

## 1.2 Systém řízení bezpečnosti informací

V této moderní době by se všechny společnosti měli zabývat řízením bezpečnosti informací. Ačkoliv se bezpečnost stala neoddelitelnou součástí řízení organizací tak mnoho organizací si neuvědomuje, že i informace jsou důležitá aktiva společnosti a i ty je nutno chránit. Aby bylo možné chránit tato aktiva cíleně, účinně a účelně je třeba se dívat na řízení bezpečnosti jako na systém.

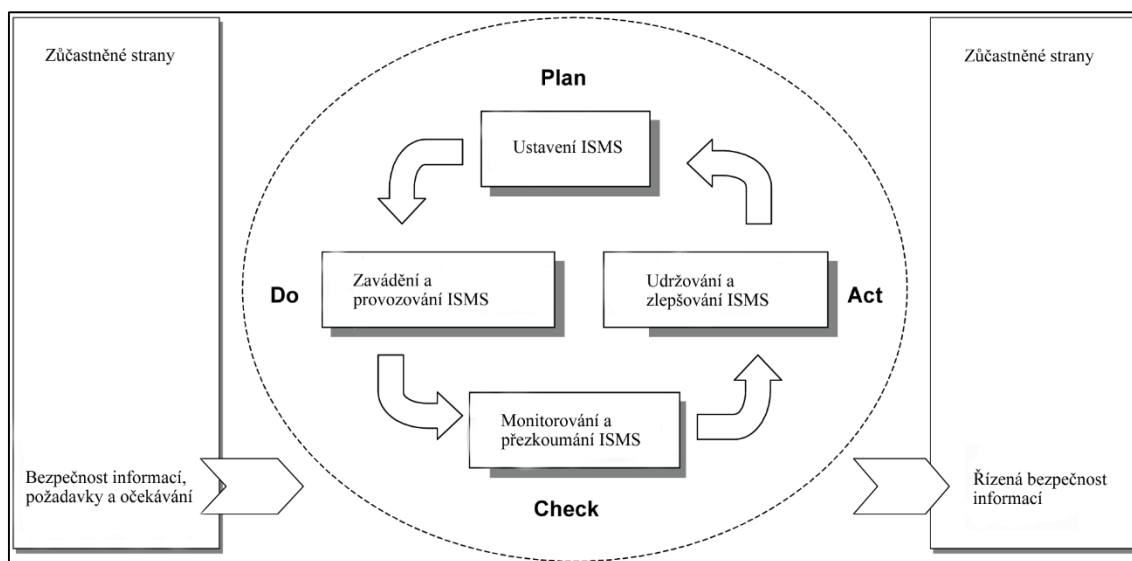
Systém řízení bezpečnosti informací (dále jen ISMS) je definován normou 27 000 jako: „ISMS sestává z politik, postupů, směrnic a příslušných zdrojů a činností, které organizace řídí, aby zajistila ochranu informačních aktiv. ISMS představuje systematický přístup k ustanovení, implementování, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací organizace tak, aby byly dosaženy její cíle.“[5, s. 18]

### 1.2.1 Model PDCA

Model PDCA vymyslel W. Edwards Deming, taky bývá označován jako Demingův cyklus, jelikož jej použil jako první ve svých pracích. Model PDCA byl původně navržen

pro inovaci a implementaci systému řízení v průmyslovém odvětví. Nyní se tento model stal základem v informační bezpečnosti, ale také se využívá jako základ pro mezinárodní standardy. Podstatou PDCA cyklu je neustálé zlepšování kvality, bezpečnosti a dalších pomocí čtyř etap, které model popisuje. Jedná se o etapy, plánuj (plan), dělej (do), kontroluj (check) a jednej (act) [2][3].

Součástí každé etapy PDCA modelu je i dokumentace. Často bývá dokumentace vnímána jako ta nejnepříjemnější a nejnáročnější součást zavádění inovace. Pomocí dokumentace je pak možné provádět různé inovace v rámci jednotlivých procesů [3].



**Obrázek 3 - Model PDCA aplikovaný na ISMS (Zdroj: Upraveno dle [4])**

Etapy PDCA cyklu aplikované na procesy ISMS:

- Plánuj (ustanovení ISMS) – v této etapě se stanovuje politika ISMS, cíle, procesy a postupy souvisejících s managementem rizik a inovace bezpečnosti informací aby bylo možné poskytovat výsledky v kooperaci s celkovou politikou a cíli organizace [4].
- Dělej (zavádění a provozování ISMS) – Zde se zavádí a využívá politika ISMS, různá opatření, postupy a procesy [4].
- Kontroluj (monitorování a přezkoumání ISMS) – Posuzujeme, tam kde je nám to umožněno jinak měříme výkon procesu k politice ISMS, cílům a praktickým zkušenostem a oznamování výsledků vedení společnosti k přezkoumání [4].

- Jednej (udržování a zlepšování ISMS) – v poslední etapě se provádí zpětná vazba k celému inovačnímu procesu. Přijmeme opatření k nápravě a preventivní opatření vzniklých na základě vnitřní kontroly ISMS a přezkoumání systému řízení vedením společnosti tak, aby bylo dosaženo neustálého zdokonalování [4].

### **1.2.2 Ustanovení ISMS**

První milníkem, který musí společnost provést je identifikace požadavků na bezpečnost informací. Tyto požadavky vychází z celkové strategie a z podnikatelských cílů společnosti s ohledem na velikost a geografickém umístění společnosti [5].

Ustanovení lze dále rozdělit na několik skupin činností, které jsou potřeba provést, než budeme ISMS zavádět.

- **Určit rozsah a hranice ISMS**

Hned na počátku je třeba si stanovit rozsah a hranice, kde se bude ISMS zavádět. Rozsah a hranice je možné aplikovat buď na celou organizační strukturu organizace, což vede k velmi vysokým nákladům na investici a může se stát, že by to v takovém rozsahu mohlo být i na škodu samotné organizaci. Druhým přístupem je určení hranic pouze na specifickou část organizace (informační systém, pobočku, organizační úsek společnosti apod.). Zaměřením se na dílčí část společnosti si snadněji obhájíme účelnost a důvody k zavedení systematického řízení bezpečnosti [1].

- **Definovat a odsouhlasit „Prohlášení o politice ISMS“**

Další činnosti, kterou je třeba provést je „Prohlášení o politice ISMS“. Toto prohlášení vzniká na základě specifických potřeb jednotlivých organizací. Prohlášení o politice ISMS by mělo obsahovat:

- Cíle ISMS a definovala základní směr
- Zohledňovala cíle a požadavky organizace
- Vytvořila potřebné vazby pro vybudování a údržbu ISMS
- Stanovit kritéria pro popis a hodnocení rizik
- Schválení vedením společnosti

Tento dokument je důležitý jelikož reprezentuje zájem vedení společnosti ohledně řízení bezpečnosti informací v podniku [5].

- **Analýza a zvládání rizik**

Analýzou rizik a jejich zvládání se budeme zabývat níže, v kapitole 1.6 analýza rizik.

- **Souhlas vedení organizace s navrhovaným zbytkovým rizikem a se zavedením ISMS**

Po provedení analýzy rizik je nutné, aby vedení organizace odsouhlasilo plán na zavedení bezpečnostních opatření pro snížení rizika a odsouhlasilo, že zbytková rizika jsou pro organizaci akceptovatelná nebo neakceptovatelná. Pokud řízení rizik nesnižuje hodnotu rizik na akceptovatelnou úroveň, je nutné modifikovat návrh bezpečnostních opatření. Tyto dva dokumenty schvalované vedením organizace jsou základní východiska pro řízení bezpečnosti informací [1].

- **Příprava „Prohlášení o aplikovatelnosti“**

Jestliže společnost potřebuje mít shodu se normou ISO/IEC 27 001 tak je tento dokument povinný. Tento dokument popisuje cíle opatření a jednotlivá bezpečnostní opatření, která byla vybrána na pokrytí existujících bezpečnostních rizik. Prohlášení o aplikovatelnosti nám poskytuje i zpětnou vazbu jelikož na základě tohoto dokumentu jsme schopni provést kontrolu, jestli jsme provedli veškerá bezpečnostní opatření nad všemi identifikovanými riziky [2].

Tyto činnosti mají následně zásadní dopad na celý životní cyklus fungování ISMS. Protože se jedná o první etapu řízení bezpečnosti informací, kde se definují základy celého ISMS se kterými následně pracujeme v dalších etapách. A změny provedené zpětně vyžadují více úsilí a jsou spojeny s většími finančními náklady, než kdyby byly provedeny řádně v této etapě [1].

### **1.2.3 Zavádění a provoz ISMS**

Zavádění a provoz ISMS je další etapou systému řízení bezpečnosti informací, která se implementují na základě navržených bezpečnostních opatření z předchozí etapy. Podstatou této etapy je potřeba připravit dílčí plány s návrhem termínů provedení, určit

odpovědné osoby a provést dokumentaci veškerých opatření. Součástí této etapy je provést ty následující činnosti [1]:

- **Definovat plán zvládnání rizik**

Tento důležitý dokument popisuje všechny činnosti v rámci ISMS, které jsou nutné pro řízení bezpečnostních rizik, stanovené cíle bezpečnosti informací, omezující faktory a potřebné zdroje. Významným prvkem, který tento plán určuje, je osoba odpovědná za provádění konkrétních činností [1].

Vytvoření plánů rizik vychází z ustanovení ISMS a podněty získané vedením organizace při pravidelném přehodnocování ISMS [1].

- **Zavést bezpečnostní opatření a zformulovat příručku bezpečnosti informací**

Při vytváření příručky bezpečnosti je nutné definovat bezpečnostní pravidla a definovat odpovědnost, která s tím souvisí. Během tvorby příručky bezpečnosti je nutné rozlišovat úrovně působení tohoto dokumentu.

Na nejvyšší úroveň (celopodnikovou) patří dokumenty, jejichž nasazení vyžaduje systémový přístup. Nebo jsou vyžadovány normou ISMS. Mezi takovéto dokumenty na nejvyšší úrovni patří rozsah, politika ISMS, zpráva o hodnocení rizik, prohlášení o aplikovatelnosti a jiné [1].

Na druhé úrovni, která slouží k prosazení a přizpůsobení konkrétnímu ISMS, je potřeba definovat do dokumentace dílčí procesy a postupy, u které budou efektivně zajišťovat prosazení dílčích bezpečnostních opatření. Tudiž je podstatné určit odpovědnou osobu, která bude vědět co, kdy kde a jak musí provádět [1].

Na nejnižší vrstvě dokumentace se musí nacházet dokumenty, které podrobně popisují jednotlivé úkony, jež jsou nezbytné pro naplnění konkrétních dílčích procesů [1].

- **Definovat program budování bezpečnostního podvědomí**

Tento program se zaměřuje na zaměstnance společnosti, jelikož si musí být vědomy politiky bezpečnosti informací v organizaci, své role v této politice, znát svůj přínos pro

efektivitu bezpečnosti informace a důsledky, pokud budou požadavky systému řízení bezpečnosti informací nedodrženy [6].

Informovanost zaměstnanců o této politice je velmi důležitá, jelikož ani veškerá bezpečnostní opatření nám nebudou fungovat správně, dokud nebudou zaměstnanci dodržovat základní bezpečnostní principy a pravidla. Proto je nutné pravidelně seznamovat nově příchozí i stálé zaměstnance s bezpečnostní politikou informace organizace [1].

- **Určit způsoby měření účinnosti bezpečnostních opatření**

Aby organizace byla schopna určit, zda je bezpečnostní opatření účelné a účinné, tak je třeba vyhodnocovat provedené opatření. Proto musí organizace zavést:

- Co je nutné monitorovat včetně procesů a opatření
- Metody monitorování, analýz a hodnocení
- Kdy se bude monitorování provádět
- Kdy budou výsledky monitorování analyzovány a vyhodnoceny
- Kdo bude výsledky analyzovat a vyhodnocovat [6]

Ukazatele, které lze měřit v rámci bezpečnosti informací je možné rozdělit na finanční, personální a technické (zde patří především ukazatele provozu IS/ICT) [1].

- **Řídit zdroje, dokumenty a záznamy ISMS**

Posledním procesem etapy zavádění ISMS je provádění všech činností řízeným způsobem. V této etapě bohužel nestačí pouze postupovat dle určených pravidel, ale je nutné sbírat podklady k další etapě. V tomto bodu je nutné, aby bylo zajištěno, že zdokumentované informace jsou kdykoliv a kdekoliv dostupné a použitelné v rámci potřeby a chráněny před prozrazením, nevhodným použitím nebo ztrátou integrity [6]. Pro další kontrolu správného fungování ISMS je nutné vytvořit pravidla pro tvorbu, schvalování, distribuci a aktualizaci dokumentace určené pro řízení bezpečnosti. U dokumentovaných informací je nutno zabezpečit distribuci, přístup, použití, ukládání, zachování (včetně čitelnosti), řízení verzí, likvidace neplatných dokumentů [1, 6].

### 1.2.4 Monitorování ISMS

Cílem této etapy účinně získávat zpětnou vazbu pomocí pravidelných přezkoumávání účinnosti opatření, kde bereme v úvahu výsledky bezpečnostních auditů, incidentů, návrhů a podnětů všech zainteresovaných stran [2].

### 1.2.5 Údržba a zlepšování ISMS

Tato etapa je poslední v celém cyklu vytváření ISMS. Cílem této etapy je udržovat a zlepšovat na základě získaných podnětů. Při výskytu neshody je nutné, aby organizace reagovala.

- Přijmout opatření k řízení a nápravě neshody
- Vyhodnotit potřebu pro opatření k odstranění příčin neshody
- Implementovat jakákoliv potřebná opatření
- Přezkoumat efektivnost každého přijatého nápravného opatření
- Provést změny v ISMS pokud je to nezbytné
- Uchovávat dokumentované informace o podstatě neshod a každého přijatého opatření
- Uchovávat dokumentované informace o výsledcích každého nápravného opatření [6]

Jelikož systém řízení bezpečnosti informací pracuje s Demingovým cyklem, tak je nutné, aby organizace neustále zlepšovala vhodnost, přiměřenost a efektivnost ISMS [6].

## 1.3 Normy řady ISO/IEC 27 00x

Mezinárodní organizace pro standardizaci určila tuto řadu pro řízení bezpečnosti informací v organizacích [5].

- **ISO/IEC 27000** Systémy řízení bezpečnosti informací - přehled a slovník
- **ISO/IEC 27001** Systémy řízení bezpečnosti informací – požadavky
- **ISO/IEC 27002** Soubor postupů pro opatření bezpečnosti informací
- **ISO/IEC 27003** Směrnice pro implementaci ISMS
- **ISO/IEC 27004** Řízení bezpečnosti informací – měření
- **ISO/IEC 27005** Řízení rizik bezpečnosti informací

- **ISO/IEC 27006** Požadavky na orgány poskytující audit a certifikaci systému
- **ISO/IEC 27007** Směrnice pro audit ISMS
- **ISO/IEC TR 27008** Směrnice pro audit opatření ISMS
- **ISO/IEC 27010** Směrnice pro ISMS pro meziodvětvové komunikace a komunikace mezi organizacemi
- **ISO/IEC 27011** Směrnice pro ISMS pro telekomunikační organizace na základě ISO/IEC 27002
- **ISO/IEC 27013** Návod pro integrovanou implementaci ISO/IEC 27001 a ISO/IEC 20000-1
- **ISO/IEC 27014** Správa bezpečnosti informací
- **ISO/IEC 27015** Směrnice pro řízení bezpečnosti informací pro finanční služby
- **ISO/IEC 27016** Řízení bezpečnosti informací – Organizační ekonomika

Řada norem ISMS	Norma obsahující terminologii	27000 Přehled a slovník		
	Normy specifikující požadavky	27001 Systém řízení bezpečnosti informací - Požadavky	27006 Požadavky na orgány poskytující audit a certifikaci systémů řízení bezpečnosti informací	
	Normy popisující obecné směrnice	27002 Soubor postupů pro opatření bezpečnosti informací	TR 27008 Směrnice pro audit opatření ISMS	
		27003 Směrnice pro implementaci systému řízení bezpečnosti informací	27013 Návod pro integrovanou implementaci ISO/IEC 27001 a ISO/IEC 20000-1	
		27004 Řízení bezpečnosti informací - Měření	27014 Správa bezpečnosti informací	
		27005 Řízení rizik bezpečnosti informací	TR 27016 Řízení bezpečnosti informací - Organizační ekonomika	
		27007 Směrnice pro audit systémů řízení bezpečnosti informací		
	Normy popisující směrnice specifické pro odvětví	27010 Směrnice pro řízení bezpečnosti informací pro meziodvětvové komunikace a komunikace mezi organizacemi	TR 27015 Směrnice pro řízení bezpečnosti informací pro finanční služby	
		27011 Směrnice pro řízení bezpečnosti informací pro telekomunikační organizace na základě ISO/IEC 27002	TR 27017 Směrnice pro opatření bezpečnosti informací při použití služeb cloud computingu na základě ISO/IEC 27002	
	Normy popisující směrnice specifické pro opatření	2703x	2704x	

Obrázek 4 - Vazby mezi normami ISMS (Zdroj: Upraveno dle [5])

### 1.3.1 Norma ISO/IEC 27000

Účelem této mezinárodní normy je poskytnutí přehledu systému řízení bezpečnosti informací a definování odborné terminologie. Využitelnost této normy je ve všech typech a velikostech organizací [5].

### 1.3.2 Norma ISO/IEC 27001

V této normě jsou definovány požadavky pro ustanovení, implementování, udržování a neustálé zlepšování ISMS v organizaci. V normě jsou dále specifikovány požadavky na posuzování a ošetření rizik bezpečnosti informací, určené pro potřeby organizací bez ohledu na typ, velikost a druh činností. Aby byla dosažena shoda s touto normou, tak musí být splněny všechny požadavky. V příloze této normy jsou stanoveny cíle opatření a jednotlivá opatření, které jsou přímo propojené normou ISO/IEC 27002 [6].

### 1.3.3 Norma ISO/IEC 27002

Tato norma obsahuje směrnice a postupy pro řízení bezpečnosti informací. V normě je zahrnut výběr, implementace a řízení opatření s ohledem na prostředí rizik bezpečnosti informací organizace. Touto normou se musí řídit ty organizace, které mají v úmyslu vybrat opatření v rámci činností zavádění ISMS založeném na normě ISO/IEC 27001 nebo zavedení obecně uznávaných opatření bezpečnosti informací nebo vytvořit vlastní směrnice k ISMS. Ve 14-ti kapitolách této normy jsou popsány opatření a celkem mají 35 kategorií bezpečnosti s 114-ti kontrolami [10].

Označení	Název kapitoly	Kategorie	Opatření
A.5	Politiky bezpečnosti informací	1	2
A.6	Organizace bezpečnosti informací	2	7
A.7	Bezpečnost lidských zdrojů	3	6
A.8	Řízení aktiv	3	10
A.9	Řízení přístupu	4	14
A.10	Kryptografie	1	2
A.11	Fyzická bezpečnost a bezpečnost prostředí	2	15
A.12	Bezpečnost provozu	7	14
A.13	Bezpečnost komunikací	2	7
A.14	Akvizice, vývoj a údržba systémů	3	13
A.15	Dodavatelské vztahy	2	5
A.16	Řízení incidentů bezpečnosti informací	1	7
A.17	Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací	2	4
A.18	Soulad s požadavky	2	8

Tabulka 1 - Kategorie opatření ISO/IEC 27002 (Zdroj: Upraveno dle [10])

### **1.3.4 Norma ISO/IEC 27003**

Norma poskytuje návrhy pro úspěšnou implementaci ISMS v souladu s ISO/IEC 27001. Norma je aplikovatelná na všechny typy a velikosti organizací, které chtějí zavádět ISMS. Je zde popsán proces návrhu a implementace ISMS na jehož konci je vytvořen finální plán. Tento plán slouží jako podklad pro realizaci projektu implementace ISMS. Tento proces implementace je v normě rozdělen do pěti etap [4]:

- a) získání souhlasu vedení organizace se zahájením projektu ISMS
- b) definování rozsahu, hranic a politiky ISMS
- c) provedení analýzy požadavků bezpečnosti informací
- d) provedení hodnocení rizik a plánování zvládnutí rizik
- e) návrh ISMS

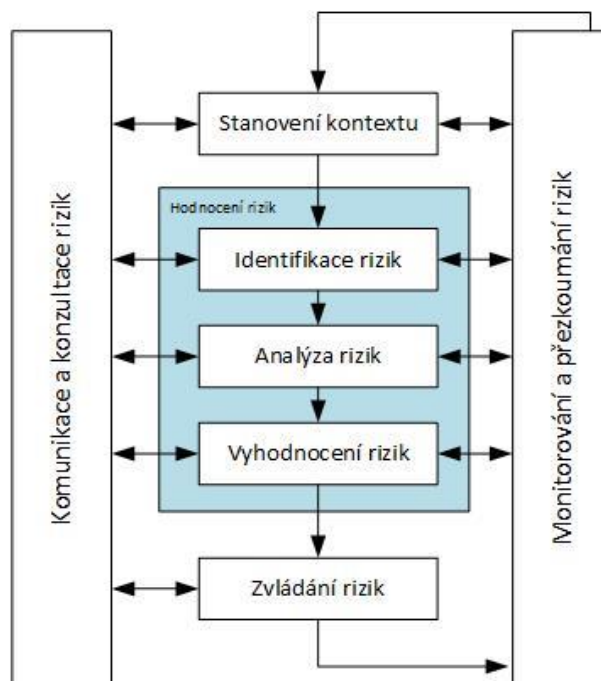
Výstupem poslední etapy je finální plán implementace projektu systému řízení bezpečnosti informací. V normě se nachází pouze doporučení a vysvětlení neurčuje žádné požadavky, které by měnily nebo redukovaly požadavky v ISO/IEC 27001 a ISO/IEC 27002 [4].

### **1.3.5 Norma ISO/IEC 27004**

Jelikož musíme měřit účinnost zavedených bezpečnostních opatření a zavedeného ISMS je nutné mít k tomu kvalitní metriky, ze kterých jsme schopni vyhodnotit jednotlivá bezpečnostní opatření nebo i skupiny těchto opatření. A právě tímto se zabývá tato norma, která nám poskytuje doporučení pro vývoj a používání metrik. Program měření bezpečnosti informací zahrnuje činnosti rozvoje metrik a měření, provádění měření, analýzu dat a hlášení výsledků měření [2].

### **1.3.6 Norma ISO/IEC 27005**

Tato norma nabízí doporučení jak řídit rizika bezpečnosti informací v rámci organizace. Norma je rozdělena tak, aby kvalitně podporovala implementaci informační bezpečnosti na základě přístupu řízení rizik. V normě není uvedena konkrétní metodika jak řídit rizika spojená s bezpečností informací, záleží čistě na organizaci, jaký přístup k řízení rizikům zvolí s ohledem na rozsah implementace ISMS či odvětví, ve kterém organizace působí. Manažeři a pracovníci, kteří jsou v rámci organizace odpovědní za řízení rizik bezpečnosti informací, by měli znát tuto normu, jelikož je určena právě pro ně [2].



Obrázek 5 - Řízení rizik (Zdroj: upraveno dle [1])

### 1.3.7 Norma ISO/IEC 27006

V normě jsou popsány požadavky a doporučení pro orgány, které provádějí audity a certifikace ISMS. Tato norma je v hlavně určena pro podporu procesů akreditace certifikačních orgánů poskytujících certifikace ISMS [2].

## 1.4 Zákony týkající se bezpečnosti informací v ČR

### 1.4.1 Zákon o elektronickém podpisu

Zákon č. 227/2000 Sb. neboli zákon o elektronickém podpisu upravuje používání elektronického podpisu, elektronické značky, poskytování certifikačních služeb a souvisejících služeb poskytovateli usazenými na území České republiky. Dále stanovuje kontrolu povinností a sankce při porušení tohoto zákona. V roce 2010 byla zavedena povinnost uvádět a zveřejňovat seznam certifikačních služeb, jejíž služby jsou důvěryhodné [1,7].

### 1.4.2 Zákon o archivnictví a spisové službě

Zákon č. 499/2004 Sb. o archivnictví a spisové službě se zaměřuje na úpravu:

- Výběr, evidenci a kategorizaci archiválií,
- Ochranu archiválií,

- Práva a povinnosti vlastníků archiválií,
- Využívání archiválií,
- Zpracování osobních údajů pro účely archiválií,
- Spisovou službu,
- Správní delikty [8].

Tento zákon byl doplněn vyhláškou č. 645/2004 Sb., která definuje pojmy dokument a archiválie. Dokumentem se rozumí každý písemný, obrázkový, zvukový, elektronický nebo jiný záznam. Nezáleží, zda je tento záznam analogový nebo digitální ale musí pocházet z činnosti původce. Archiválie je na základě této vyhlášky chápána jako záznam, který je nutné trvale uchovat. Mezi archiválie patří i pečeti a razítka [1].

#### **1.4.3 Zákon o ochraně osobních údajů**

Zákon č. 101/2000 Sb. o ochraně osobních údajů stanovuje v souladu s evropským právem a mezinárodními smlouvami, kterými je Česká republika vázaná a k naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí. Dále upravuje práva a povinnosti při zpracovávání osobních údajů a stanovuje podmínky, během kterých se provádí předání osobních údajů do jiných států. Na základě tohoto zákona je zřízen Úřad pro ochranu osobních údajů [9].

#### **1.4.4 Zákon o kybernetické bezpečnosti**

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti nabyt účinnost od 1. 1. 2015. Tento zákon vznikl na základě směrnice evropské unie, která požaduje, aby všechny státy evropské unie zvýšili svou schopnost vzdorovat případným útokům na kybernetické úrovni a tím ochránit kritické obory pro bezpečný a bezchybný chod státu. Do těchto oborů patří ekonomika jako celek, energetika, doprava a další strategická odvětví, která závisí na IT systémech. Na základě tohoto zákona by se měla sjednotit elektronická komunikace, která probíhá nejen ve státní správě, ale i ve sféře soukromé. Národní centrum kybernetické bezpečnosti se sídlem v Brně má podle zákona kontrolní a výkonnou moc. Účinností tohoto zákona by Česká republika měla být schopná jednodušeji rozpoznat ale i aktivně bojovat s útoky na kybernetické systémy v České republice. Platnost zákona má zlepšit ochranu i osobních dat občanů, kteří jsou vedení na jednotlivých úřadech, bankách nebo jiných databázích [11].

Zákon o kybernetické bezpečnosti se velmi podobá normě ISO/IEC 27001 o systému řízení bezpečnosti informací [12].

Sněmovna k tomuto zákonu schválila ještě prováděcí předpisy, které byly převzaty od Národního bezpečnostního úřadu, tak aby tento zákon mohl opravdu zvyšovat bezpečnost a chránit IT systémy v České republice [13].

- Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (předpis č.316/2014 sb. vyhláška o kybernetické bezpečnosti)
- Vyhláška o významných informačních systémech a jejich určujících kritériích (Předpis č. 317/2014 Sb.)
- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

Vyhláška o kybernetické bezpečnosti určuje, jak musí povinné subjekty jednat, ale neurčuje, které budou patřit do významných a kritických informačních infrastruktur. Kritéria pro určení významné a kritické infrastruktury určují druhý a třetí prováděcí předpis, jež jsou zmíněny výše [13].

Vyhláška o významných informačních systémech a jejich určujících kritériích určuje, které informační systémy jsou těmi významnými, a definuje pravidla na základě, kterých je možné určit, zda bude posuzovaný informační systém tím významným [14]:

- oběti na životech s mezní hodnotou více než 10 mrtvých nebo 100 zraněných osob vyžadující lékařské ošetření, s případnou hospitalizací delší než 24 hodin,
- finanční nebo materiální ztráty s mezní hodnotou více než 5% stanoveného rozpočtu orgánu veřejné moci,
- zásah do života postihující nejméně 50 000 osob,
- výrazné ohrožení nebo narušení veřejného zájmu.

Informační a komunikační systémy kritické informační infrastruktury mohou být podle nařízení vlády vlastněny soukromými vlastníky, ale i zde patří systémy veřejné správy.

Nařízení vlády pouze obsahuje kritéria, která musí být splněna, aby takovýto systém byl prvkem kritické informační infrastruktury [13, 15]:

- obětí s mezní hodnotou více než 250 mrtvých nebo více než 2500 osob s následnou hospitalizací po dobu delší než 24 hodin,
- ekonomického dopadu s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % HDP,
- dopad závažného zásahu do každodenního života postihujícího více než 125 000 osob.

V příloze nařízení vlády se nachází odvětvová kritéria na základě, kterých lze určit, zda prvek patří do kritické infrastruktury. Jsou zde uvedeny podmínky pro energetiku (výroba elektřiny nad 500MW), zdravotnictví (alespoň 2500 akutních lůžek), komunikační a informační systémy (řídící a datová centra) a další [15].

Opatření, která jsou v kybernetickém zákoně zmíněna, pro zajištění kybernetické bezpečnosti jsou rozdělena na technické a organizační. Do organizačních opatření patří především systém řízení bezpečnosti informací, který musí být plně podporován vedením společnosti. Další důležité opatření patří i bezpečnost lidských zdrojů. Zde patří školení zaměstnanců, které by nemělo být jednorázové a krátkodobé nýbrž systematické, srozumitelné a pravidelné. Ostatními organizačními opatřeními jsou například [12, 16]:

- řízení rizik
- bezpečnostní politika
- organizační bezpečnost
- stanovení bezpečnostních požadavků pro dodavatele
- řízení aktiv

Do technických opatření patří [16]:

- fyzická bezpečnost
- nástroj pro ochranu integrity komunikačních sítí
- nástroj pro ověřování identity uživatelů

- nástroj pro řízení přístupových oprávnění
- nástroj pro ochranu před škodlivým kódem
- aplikační bezpečnost
- a další

Orgány a osoby, na které se vztahuje kybernetický zákon, jsou povinny zajistit bezpečnostní opatření pro informační a komunikační systém kritické informační infrastruktury nebo významný IS a vést o nich bezpečnostní dokumentaci. Dále jsou povinny zohledňovat požadavky na bezpečnostní opatření při výběru dodavatele informačního systému kritické informační infrastruktury. Subjekty, na které se vztahuje kybernetický zákon, jsou povinni hlásit kybernetické bezpečnostní incidenty v jejich síti Národnímu centru kybernetické bezpečnosti [16].

## **1.5 Analýza aktiv**

Jak už jsem psal výše tak aktiva jsou veškerým majetkem firmy. Aktiva můžeme dělit na hmotné (server, tiskárna) nebo nehmotné (software, licence). Podle ISMS dalším dělením aktiv je na primární (informace, know-how), převážně nehmotného charakteru, a sekundární (technické vybavení, síťová infrastruktura), převážně hmotného charakteru [2].

Proto, abychom je mohli ohodnotit, je musíme nejprve identifikovat. U tohoto kroku je vhodné jednotlivé aktiva seskupit podle firemní oblasti kam patří (bezpečnostní aktiva, programová aktiva, fyzická aktiva a další). Po identifikování aktiva firmy je třeba určit i vlastníka daného aktiva, který bude dané aktivum spravovat a bude za něj plně odpovědný [2].

### **1.5.1 Hodnocení aktiv**

K hodnocení aktiv je třeba konzultovat jednotlivé aktiva s vlastníkem a s tím kdo dané aktivum používá, aby se zachovalo objektivnost hodnocení. Nebo můžeme využít softwarové řešení využívající metodiku CRAMM. K hodnocení je důležité sestavit si tabulku, na základě které budou hodnotit jednotlivá aktiva. Stupnice hodnocení aktiv může být číselná (1-5, vyjádření v penězích) nebo slovní (zanedbatelná až velmi kritická), obě tyto varianty se dají zkombinovat. K nejjednoduššímu ohodnocení aktiv se používá vzorec:

(Důvěrnost + Dostupnost + Integrita)/3

Jelikož porušením jedné z těchto tří položek nám rostou případné náklady na poničení daného aktiva [2].

Číselné ohodnocení aktiv	Slovní hodnocení aktiv	Dopad na firmu
1	Zanedbatelná	Nulový dopad
2	Malá	Malý dopad může mít nepříznivý vliv na chod firmy, ale neprojeví se v poskytovaných službách navenek
3	Významná	Střední dopad, může znamenat větší finanční výdaje a šíření negativních zpráv o firmě
4	Cenná	Vážný dopad veřejně špatná image firmy, nedůvěra našich klientů, žaloby za ztrátu důvěrnosti
5	Velmi cenná	Existenční problémy platební neschopnost firmy, neudržitelné stav podnikání

Tabulka 2 - Hodnocení aktiv (Zdroj: upraveno dle [2])

## 1.6 Analýza rizik

Analýza rizik je další důležitý bod při řízení bezpečnosti informací. Jelikož jsme si vědomi rizika a následných bezpečnostních hrozeb, která na nás mohou působit, tak jsme schopni určit a implementovat bezpečnostní opatření, které nám sníží bezpečnostní hrozbu na přijatelnou úroveň a dopad daného rizika bude minimalizován. Abychom mohli efektivně a účelně vynakládat náklady na bezpečnost informací a zvyšovali tím efektivnost společnosti tak je důležité provést analýzu rizik důsledně [2].

Při vyhodnocování rizik vycházíme z pravděpodobností vzniku rizika (P) a míry rizika (R) Stupnice pravděpodobnosti vzniku rizika a jeho existence může mít pět hodnot nahodilá, nepravděpodobná, pravděpodobná, velmi pravděpodobná a trvalá [2].

Stupnice míry rizika může také mít pět hodnot[2]:

- **Zanedbatelné riziko** – nejedná se o 100% bezpečnost, ale není třeba zavádět bezpečnostní opatření.

- **Akceptovatelné riziko** – náklady na zavedení opatření mohou převyšovat hodnotu aktiva, je tedy nutné zvážit zavedení opatření vedením organizace.
- **Mírné riziko** – bezpečnostní opatření je nutné zavádět na základě zpracovaného plánu na základě rozhodnutí vedení organizace. Opatření snižující rizika musí být dle plánu implementována.
- **Nežádoucí riziko** – Bezpečnostní opatření snižující toto riziko na přijatelnou úroveň musí být urychleně provedeno s dostatečnými zdroji na provedení. Aby se přesněji stanovila pravděpodobnost vzniku incidentu, je třeba provést další vyhodnocování, aby již riziko nebylo spjato s velkými následky.
- **Nepřijatelné riziko** – nutnost okamžitého zastavení činnosti a implementovat bezpečnostní opatření dokud se hodnota rizika nesníží. Opatření se může na základě vyhodnocování implementovat více.

### 1.6.1 Metodiky analýzy rizik

Analýzu rizik je možné rozdělit na několik úrovní na základě použité metodiky. Nejvíce doporučovanou kombinací použitých metodik je metoda pragmatická (neformální) a následně metoda pro detailní analýzu rizik.

Jako první by měla být provedena analýza na hrubé úrovni, která nám identifikuje systémy, které jsou pro naši činnost organizace důležité nebo jsou vystaveny vysokým rizikům, provádíme podrobnou analýzu [2].

Metodiky pro analýzu rizik:

- Hrubá úroveň
- Neformální přístup
- Kombinovaný přístup
- Podrobný přístup

#### Analýza na hrubé úrovni

Hrubou úrovní je myšlen pohled na celou činnost organizace (jaká je hodnota IT systému a zpracování informací a rizika). Na základě následujících skutečností se rozhodne, jaký bude ideální přístup pro IT systém [2]:

- Jakých cílů má být dosaženo, použijeme-li daný IT systém

- Jaké budou investice do vývoje, údržby IT systému případně jeho nahrazení
- Jaká jsou aktiva IT systému, kterých jsou pro organizaci důležitá
- Jak jsou jednotlivé činnosti organizace závislé na systému IT

Na základě tohoto rozdělení bude organizace vědět, jaké systémy jsou méně kritické, nákladné nebo jsou více kritické pro chod organizace a je třeba u těchto systémů provést podrobnou analýzu rizik [2].

### **Neformální analýza**

Tato analýza vychází ze znalostí a zkušeností jednotlivců. Mezi největší výhody této analýzy je, že se není třeba učit nových dovedností a není příliš náročná na zdroje a čas. Na základě rychlejšího zpracování neformální analýzy a bez detailních seznamů kontrol roste pravděpodobnost, že dojde k opomenutí důležitých detailů než tomu je u podrobného přístupu. Z tohoto důvodu je náročné obhájit zavedení ochranných bezpečnostních opatření na základě bezpečnostních rizik, které byly určeny tímto způsobem [2].

### **Kombinovaný přístup**

Tento přístup umožňuje kombinaci nejlepších charakteristik možností a umožňuje minimalizovat čas a úsilí věnované na identifikaci ochranných opatření. Jako první se u tohoto přístupu provede analýza IT systému na hrubé úrovni. U systému, kdy jsou identifikována vysoká rizika nebo patří jako významné činnosti organizace, je provedena podrobná analýza rizik. U ostatních IT systému je následně proveden pouze základní přístup [2].

### **Podrobný přístup**

Podrobný přístup nebo též detailní analýza rizik umožňuje hloubkovou analýzu rizik IT systému, která obsahuje identifikaci souvisejících rizik a odhad jejich velikosti. Aby byla hloubková analýza rizik úspěšná, postupuje podle následujících kroků [2]:

- **Stanovení hranic revize**

Musíme určit hranice, ve kterých se bude provádět analýza rizik. Určením hranic se předejde provádění zbytečných činností [2].

- **Identifikace aktiv**

Aktivum je dílčí část celkového systému případně jeho díl systému, kterému organizace přiřadila určitou hodnotu. Jelikož z dílčí části se tvoří celky je nutné s touto logikou provádět celou identifikaci aktiv [2].

- **Ohodnocení aktiv**

Po identifikaci aktiv je nutné je ohodnotit. Ohodnocení probíhá podle schématu, které se v organizaci stanoví. Toto schéma rozděluje aktiva podle toho, jakou mají jednotlivá aktiva hodnotu pro organizaci. Hodnota aktiva nemusí být definována jen podle finančního ohodnocení, ale i z podle negativních dopadů na provoz organizace na základě ztráty důvěrnosti, integrity nebo dostupnosti [2].

- **Hodnocení hrozeb**

Jelikož hrozby umožňují poškodit aktivum organizace tak se stanovuje seznam hrozeb, které mohou vzniknout na aktivech působením lidského nebo přírodního faktoru. Hrozby mohou být náhodné nebo úmyslné. Hrozby jsou hodnoceny na základě aktiv organizace [2].

- **Odhad zranitelnosti**

Definuje slabá místa v bezpečnosti informací v organizaci ať už ve fyzickém prostředí, firemních postupech, personálu, správou IT/ICT. Slabá místa vznikají působením hrozby na aktivu, kde mohou způsobit škodu [2].

- **Identifikace plánovaných a existujících ochranných opatření**

Při provádění analýzy rizik je nutné identifikovat jaká ochranná opatření, která jsou již v organizaci zavedeny, nebo se plánují zavést. Výsledkem je pak seznam již zavedených ochranných opatření [2].

- **Výběr ochranných opatření**

Výběr jednotlivých opatření se provádí, aby se snížilo riziko. Mezi nejdůležitější kategorie ochranných opatření patří řízení a politiky bezpečnosti IT, řešení incidentů, personální opatření, provozní plány a fyzická bezpečnost [2].

- **Odhad rizik**

Aktiva společnosti jsou vystavena různým rizikům. V odhadu rizik se určují, jaká rizika nám hrozí a z jakého důvodu nám tato rizika hrozí [2].

- **Přijetí rizik**

Přijetí rizik probíhá po aplikování jednotlivých opatření na identifikovaná rizika. A jestliže existují zbytková rizika po aplikování opatření tak můžeme rozhodnout, že budeme aplikovat nová bezpečnostní opatření nebo můžeme zbytkové riziko akceptovat [2].

- **Politika bezpečnosti systému IT**

Politika bezpečnosti IT systémů by měla obsahovat detailní popis jednotlivých opatření a jejich důvod proč jsou tato opatření nezbytná [2].

- **Plán bezpečnosti**

Plán bezpečnosti je dokument, ve kterém jsou popsány všechny činnosti, které musí být provedeny, aby všechny navržené bezpečnostní opatření mohla být implementována [2].

### **1.6.2 Řízení rizik**

Důvodem, proč řídíme rizika je jejich snížení či úplná eliminace. Řízení rizik je ucelený proces, který se skládá z několika činností:

**Stanovení kontextu**, ve které se stanoví oblast pro řízení rizik, výběr metodiky pro analýzu rizik, kritéria a způsob při hodnocení a zvládání rizik [2].

**Analýza rizik**, identifikuje a kvantifikuje aktiva, hrozby, zranitelnost a určuje míru rizika [2].

**Vyhodnocování rizika**, zde se určují priority pro jednotlivá rizika a určení optimálního opatření pro snížení hodnoty rizika [2].

**Zvládání rizik** je poslední činnosti při řízení rizik, ve které se určuje, jakým způsobem budeme snižovat riziko. Možnosti jakými lze zvládat rizika jsou retence, redukce, pojištění, sdílení nebo vyhnutí se riziku [2].

## **2 ANALÝZA SOUČASNÉHO STAVU**

Tato kapitola se bude věnovat základním údajům o vybrané firmě, dále o analýze aktuálního stavu hardwaru, softwaru, bezpečnosti informací ve firmě. Veškeré informace jsem získal na základě konzultace se zaměstnanci a majitelkou, která souhlasila s poskytnutím firemních údajů výměnou za anonymitu její společnosti.

### **2.1 Informace o podniku**

Firma ABC se zaměřuje zpracování podvojného účetnictví, daňovou evidenci, kontrolu účetnictví, vypracování daňových přiznání a poskytuje i poradenství v oblasti účetnictví a daní. Firma ABC provozuje svou činnost od roku 2010 a od té doby se jí podařilo získat klienty od osob samostatně výdělečně činných až po malé organizace.

Firma sídlí v pronajatých kancelářských prostorách o čtyřech místnostech. Kanceláře se nachází v nejvyšším patře budovy. Dvě místnosti jsou vyhrazeny pro pět zaměstnanců, v jedné místnosti sídlí majitel firmy ABC a z třetí místnosti udělali archiv pro dokumenty a umístili zde server.

### **2.2 Bezpečnost ve firmě**

Firma se zatím nezabývala zavedením systému řízení bezpečnosti informací ani nijak neřešili bezpečnost IT/ICT v organizaci.

#### **2.2.1 Fyzická bezpečnost v podniku**

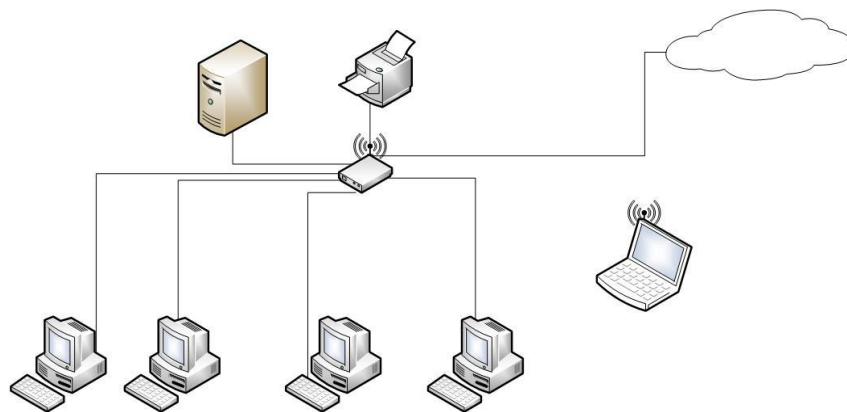
Vstup do budovy se od 17 hodin do 7 hodin zamyká, jinak je po zbytek dne otevřený. Hlavní vstup do kanceláří je zajištěn bezpečnostními dveřmi, které zamyká poslední zaměstnanec při odchodu. Každý zaměstnanec má klíče od hlavních dveří a vstupu do kanceláře. Jednotliví zaměstnanci dále mají klíče od kanceláře, ve které pracují. Do archivu má přístup pouze majitelka firmy.

#### **2.2.2 IS/ICT v podniku**

Firma vlastní pět stolních počítačů pro zaměstnance a jeden notebook pro majitele firmy. Na těchto zařízeních je nainstalován operační systém Windows 7, kancelářský balík MS Office 2013 a o bezpečnost se stará antivirový program Eset secure office+, kde probíhají pravidelné aktualizace virové databáze. Každá pracovní stanice je zabezpečena osobním heslem daného zaměstnance. Jednotlivé pracovní stanice jsou propojeny UTP kabelem

k podnikové síti. Podniková síť umožňuje taky připojit se pomocí technologie Wi-Fi především majitele firmy. Wi-Fi je zabezpečeno pomocí šifrování WPA2 s použitím silného hesla. Router je kvůli bezpečnosti umístěn v archívu firmy. Součástí routeru je i firewall, jehož nastavením se nikdo v organizaci ani externí IT společnost nezabývala. Připojení k internetu je zabezpečeno pomocí kabelového připojení. Vedení kabelových tras je uloženo ve žlabech, aby nedošlo k jejich poškození.

Organizace vlastní server společnosti Dell, na které je operační systém Windows server 12 a nainstalovaný informační systém Helios. O bezpečnost na serveru se stará antivirus společnosti ESET, který se pravidelně aktualizuje. K serveru se připojují jednotliví uživatelé přes vzdálený uživatelský přístup. Přístup v informačním systému není nijak omezený na základě uživatelských jmen. Takže všichni zaměstnanci mají přístup k důvěrným datům jednotlivých klientů zaměstnavatele.



**Obrázek 6 - Schéma podnikové sítě (Zdroj: vlastní zpracování)**

Prezentace firmy na internetu je zajištěna pomocí webové stránky, která je uložena na serveru dodavatele. Organizace dále využívá služeb IT společnosti pro správu IT/ICT v organizaci.

Zálohování dat se v organizaci řeší velmi volně většinou je spojeno na základě odevzdávání příznání k dani z přidané hodnoty klienta, což je jednou za měsíc nebo za čtvrtletí. Vždy se zálohují data pouze těchto klientů. Neprovádí se žádné zálohy spojené s nastavením různých zařízení apod. Data klientů se vypálí na běžné DVD, které jsou následně uložena do police v archívu.

### 2.2.3 Bezpečnostní politika ve firmě

Jelikož organizace pracuje s důvěrnými informacemi mnoha firem. Tak každý zaměstnanec je na začátku svého pracovního poměru seznámen se svými právy a povinnostmi. Mezi povinnostmi, které zaměstnavatel vyžaduje, je kladen důraz na dohodu o mlčenlivosti tak aby nedocházelo k únikům informací třetím stranám. A firma tak nepřišla o stávající, ale i nové zakázky. Dohoda o mlčenlivosti se vztahuje i na zaměstnance, kteří již ve firmě nepracují.

Vedení organizace zatím systém řízení bezpečnosti informací nijak neřešilo. A jednotliví zaměstnanci nemají nijak omezen přístup k serveru či informačního systému na něm nainstalovaný. Dále zaměstnanci nemají jakékoliv omezení při práci na osobních stanicích.

## 2.3 Identifikace aktiv

Druh aktiva	aktiva
Hmotné	Počítače a notebook
	Server
	Tiskárny
	Kabeláž a aktivní prvek
Nehmotné – software	Informační systém
	Operační systémy
Data	O zaměstnancích
	Databáze klientů
	Zálohy dat
	Fyzické účetní doklady klientů
	Elektronické účetní doklady
	Pracovní výkazy
Služby	Připojení k internetu
	Telefonní služby

Tabulka 3 - Identifikace aktiv (Zdroj: Vlastní zpracování)

### 2.3.1 Klasifikace aktiv

Na základě identifikovaných aktiv organizace, byla po konzultaci s majitelkou organizace stanovena klasifikační schéma aktiv. Aktiva byla rozdělena do čtyř kategorií.

Jednotlivé kategorie byly stanoveny, podle toho jak jsou aktiva v organizaci ceněna od zanedbatelných po velmi cenná.

<b>Číselné ohodnocení aktiv</b>	<b>Slovní hodnocení aktiv</b>	<b>Význam ohodnocení aktiv</b>
1	Zanedbatelná	Nulový dopad, lehce nahraditelná aktiva, velmi nízké náklady na výměnu.
2	Malá	Aktiva mají už nějakou cenu, jejich náhrada nemusí být okamžitá, jelikož nedojde k ohrožení poskytování služeb navenek organizace.
3	Významná	Střední dopad, může znamenat větší finanční výdaje a šíření negativních zpráv o firmě, nedůvěru klientů
4	Velmi cenná	Vážný dopad, který může způsobit existenční problémy, platební neschopnost firmy, zánik organizace.

Tabulka 4 - Klasifikace aktiv v organizaci (Zdroj: vlastní zpracování)

### 2.3.2 Ohodnocení aktiv

Jednotlivým aktivům byla přiřazena hodnota z klasifikačního schématu aktiv. Tato hodnota vznikla, byla určena na základě průměru důvěrnosti, integrity a dostupnosti aktiva.

<b>Druh aktiva</b>	<b>aktiva</b>	<b>Hodnota aktiva</b>
Hmotné	Počítače a notebook	3
	Server	4
	Tiskárny	1
	Síťová infrastruktura	3
	Aktivní prvky	2
Nehmotné – software	Informační systém Helios	4
	Kancelářský software	3
	Operační systém	3
	Informační	O zaměstnancích

	Databáze klientů	2
	Zálohy dat	3
	Fyzické účetní doklady klientů	3
	Elektronické účetní doklady	3
	Pracovní výkazy	2
Služby	Připojení k internetu	2
	Telefonní služby	1

Tabulka 5 - Ohodnocení aktiv firmy (Zdroj: Vlastní zpracování)

## 2.4 Identifikace hrozeb

Podobně jako byla klasifikační stupnice u aktiv tak se musí stanovit i zde klasifikační stupnice pro hrozby. To je rozděleno na dvě části, nejprve pro jednotlivé hrozby stanovíme klasifikační schéma podle pravděpodobnost vzniku dané hrozby.

Hodnota pravděpodobnosti	Popis pravděpodobnosti
1	Malá pravděpodobnost
2	Střední pravděpodobnost
3	Vysoká pravděpodobnost

Tabulka 6 - Pravděpodobnostní klasifikace hrozeb (Zdroj: vlastní zpracování)

Následně dané hodnoty pravděpodobnosti přiřadíme jednotlivým hrozbám, které jsme identifikovali.

	Hrozba	Pravděpodobnost vzniku
Fyzické hrozby	Požár	1
	Zatopení	1
	Neoprávněný vstup do kanceláří	2
Chyba technického vybavení	Poškození počítače	3
	Poškození serveru	3
	Poškození aktivních prvků sítě	2
	Výpadek připojení k internetu > 4h	1
	Poškození síťové infrastruktury	1
	Výpadek el. Proudů > 4h	2

Chyby SW	Bezpečnostní chyby OS	2
	Chyby v informačním systému	3
Interní hrozby	Chybně zaslané důvěrné informace	2
	Chyba uživatele	3
	Únik přihlašovacích údajů	3
	Ztráta fyzických dat	2
	Poškození zálohovacích médií	3
	Zavirování PC	3
	Porušení mlčenlivosti	1
Externí hrozby	Hacknutí počítače/serveru	2
	Krádež notebooku majitele	3
	Krádež zařízení	2
	Krádež citlivých dat	2

**Tabulka 7 - Pravděpodobnost vzniku hrozeb (Zdroj: vlastní zpracování)**

Dále bude vytvořena matice zranitelnosti. Tato matice bude sloučením tabulek ohodnocení aktiv (tabulka č. 5) a pravděpodobnost vzniku hrozeb (tabulka č. 7). Na základě působení hrozeb na aktiva se vytvoří hodnota, jak moc hrozba působí na aktivum na stupnici 1-5.

<b>Hodnota zranitelnosti</b>	<b>Popis zranitelnosti</b>
1	Žádný riziko
2	Minimální riziko
3	Střední riziko
4	Vysoké riziko
5	Nepříjemné riziko

**Tabulka 8 - Hodnocení rizik (zdroj: vlastní zpracování)**

	popis aktiva	Počítače a notebook	Server	Tiskárny	Síťová infrastruktura	Aktivní prvky	Informační systém	Kancelářský software	Operační systém	Data zaměstnanců	Databáze klientů	Zálohy dat	Fyzické účetní doklady klientů	Elektronické účetní doklady	Pracovní výkazy	Připojení k internetu	Telefonní služby
	hodnota aktiva	3	4	1	3	2	4	3	3	3	2	3	3	3	2	2	1
Popis hrozby	Pravděpodobnost																
Požár	2	5	5	2	5	2	4	2	3	5	4	5	5	4	5	3	2
Zatopení	1	5	5	2	2	2	3	2	2	3	2	4	5	3	2	1	1
Neoprávněný vstup do kanceláří	2	4	4	2	1	1	1	1	1	3	3	4	4	2	2	1	1
Poškození počítače	3	4	1	1	2	1	2	3	3	1	1	1	1	3	1	1	1
Poškození serveru	3	1	5	1	3	1	4	1	1	1	2	1	1	5	1	1	1
Poškození aktivních prvků sítě	2	3	5	2	2	3	2	1	1	1	1	1	1	1	1	5	1
Výpadek připojení k internetu > 4h	1	3	4	2	2	2	1	1	2	1	1	1	1	1	1	4	3
Poškození síťové infrastruktury	1	4	4	3	5	3	2	1	1	1	1	1	1	1	1	5	1
Výpadek el. Proudu > 4h	2	5	5	3	2	4	5	4	4	1	1	1	1	1	1	5	1
Bezpečnostní chyby OS	2	4	4	1	1	1	3	3	4	1	1	1	1	1	1	2	1
Chyby v informačním systému	3	2	2	1	1	1	5	2	1	4	3	1	1	5	1	1	1
Chybně zasláné důvěrné informace	2	1	1	1	1	1	1	1	1	4	4	1	1	4	1	1	1
Chyba uživatele	3	4	5	3	2	2	4	3	4	2	2	4	4	3	1	1	1
Únik přihlašovacích údajů	3	4	5	1	1	2	3	1	4	1	1	1	1	4	1	3	1
Ztráta fyzických dat	2	1	1	1	1	1	1	1	1	3	3	2	4	1	2	1	1
Poškození zálohovacích médií	3	1	1	1	1	1	1	1	1	3	3	5	1	4	1	1	1
Zavirování PC	3	3	4	1	2	2	3	2	4	3	3	1	1	4	1	2	1
Porušení mlčenlivosti	1	1	1	1	1	1	1	1	1	3	2	1	5	1	2	1	1
Hacknutí počítače/serveru	3	4	5	1	1	3	4	3	4	3	4	1	1	5	1	1	1
Krádež notebooku	3	3	1	1	1	1	1	1	1	2	4	1	1	3	1	1	1
Krádež zařízení	2	5	5	2	2	2	1	1	1	3	4	3	4	1	2	1	1
Krádež citlivých dat	2	1	1	1	1	1	1	1	1	3	4	4	5	5	2	1	1

Tabulka 9 - Matice zranitelnosti (Zdroj: vlastní zpracování)

### 2.4.1 Klasifikace rizik

Je nutné stanovit klasifikační schéma pro rizika, abychom zjistili, která rizika patří mezi vážná nebo zanedbatelná. V tabulce č. 10 je znázorněna rozdělení rizik po konzultaci s majitelkou organizace.

Riziko	Hranice rizika
Malé	0-20
Střední	21-40
Vysoké	41-60

Tabulka 10 - Klasifikace rizik (Zdroj: vlastní zpracování)

### 2.4.2 Matice rizik

	popis aktiva	Počítače a notebook	Server	Tiskárny	Síťová infrastruktura	Aktivní prvky	Informační systém	Kancelářský software	Operační systém	Data zaměstnanců	Databáze klientů	Zálohy dat	Fyzické účetní doklady klientů	Elektronické účetní doklady	Pracovní výkazy	Připojení k internetu	Telefonní služby
	hodnota aktiva	3	4	1	3	2	4	3	3	3	2	3	3	3	2	2	1
	popis hrozby																
	Pravděpodobnost																
Požár	2	30	40	4	30	8	32	12	18	30	16	30	30	24	20	12	4
Zatopení	1	15	20	2	6	4	12	6	6	9	4	12	15	9	4	2	1
Neoprávněný vstup do kanceláří	2	24	32	4	6	4	8	6	6	18	12	24	24	12	8	4	2
Poškození počítače	3	36	12	3	18	6	24	27	27	9	6	9	9	27	6	6	3
Poškození serveru	3	9	60	3	27	6	48	9	9	9	12	9	9	45	6	6	3
Poškození aktivních prvků sítě	2	18	40	4	12	12	16	6	6	6	4	6	6	6	4	20	2
Výpadek připojení k internetu > 4h	1	9	16	2	6	4	4	3	6	3	2	3	3	3	2	8	3
Poškození síťové infrastruktury	1	12	16	3	15	6	8	3	3	3	2	3	3	3	2	10	1
Výpadek el. Proudu > 4h	2	30	40	6	12	16	40	24	24	6	4	6	6	6	4	20	2

Bezpečnostní chyby OS	2	24	32	2	6	4	24	18	24	6	4	6	6	6	4	8	2
Chyby v informačním systému	3	18	24	3	9	6	60	18	9	36	18	9	9	45	6	6	3
Chybně zaslané důvěrné informace	2	6	8	2	6	4	8	6	6	24	16	6	6	24	4	4	2
Chyba uživatele	3	36	60	9	18	12	48	27	36	18	12	36	36	27	6	6	3
Únik přihlašovacích údajů	3	36	60	3	9	12	36	9	36	9	6	9	9	36	6	18	3
Ztráta fyzických dat	2	6	8	2	6	4	8	6	6	18	12	12	24	6	8	4	2
Poškození zálohovacích médií	3	9	12	3	9	6	12	9	9	27	18	45	9	36	6	6	3
Zavirování PC	3	27	48	3	18	12	36	18	36	27	18	9	9	36	6	12	3
Porušení mlčenlivosti	1	3	4	1	3	2	4	3	3	9	4	3	15	3	4	2	1
Hacknutí počítače/serveru	3	36	60	3	9	18	48	27	36	27	24	9	9	45	6	6	3
Krádež notebooku majitele	3	27	12	3	9	6	12	9	9	18	24	9	9	27	6	6	3
Krádež zařízení	2	30	40	4	12	8	8	6	6	18	16	18	24	6	8	4	2
Krádež citlivých dat	2	6	8	2	6	4	8	6	6	18	16	24	30	30	8	4	2

Tabulka 11 - Matice rizik (Zdroj: vlastní zpracování)

## 2.5 Shrnutí analýzy

Analýza současného stavu ukázala, že zaměstnanci nemusí dodržovat téměř žádné směrnice ohledně systému řízení bezpečnosti informací, jelikož v organizaci nejsou. Všichni zaměstnanci mají přístup k informačnímu systému organizace a ke všem údajům klientům, kterým zpracovávají účetní agendu. Fyzická bezpečnost organizace je dostačující. Zaměstnanci mohou jakkoliv manipulovat s osobními počítači což výrazně zvyšuje možnost narušení bezpečnosti informací. V následující kapitole se pokusím eliminovat nebo alespoň snížit tato rizika na přijatelnou úroveň.

## 3 NÁVRH ŘEŠENÍ

V této kapitole je popsán postup zavedení systému řízení bezpečnosti informací ve vybrané společnosti podle řady norem ISO 27000. Na základě analýzy současného stavu je nutné snížit rizika, která budou mít velký dopad na firmu. Cílem této kapitoly vypracování návrhu bezpečnostní příručky, ve které budou popsána jednotlivá opatření pro eliminaci rizik nebo alespoň jejich redukci na akceptovatelnou úroveň.

### 3.1 Zavedení ISMS

#### 3.1.1 Rozsah zavedení ISMS

System řízení bezpečnosti informací bude mít rozsah na veškerý HW, SW, zaměstnance. Jelikož se jedná o malou společnost, kde musí mít všichni zaměstnanci přístup k SW, aby vůbec mohli vykonávat svou práci tak rozsah ISMS byl určen majitelkou na celou její organizaci.

#### 3.1.2 Soubor opatření

V následující tabulce jsou vypsána všechna opatření podle normy ISO/IEC 27001. U každého opatření je uvedeno, zda se má *zavést*, *aktualizovat* nebo *ignorovat* z důvodu, že se společnost danou oblastí nezabývá (např. vývoj IS) a tudíž se ani nenachází ve společnosti. Jistá opatření již byla zavedena, ale z důvodů aktuálnosti bylo rozhodnuto, že se i zavedená opatření se aktualizují při vytváření ISMS.

Označení	Název opatření	Stav
A.5	Politiky bezpečnosti informací	
A.5.1	Směrování bezpečnosti informací vedením organizace	
A.5.1.1	Politiky pro bezpečnost informací	<i>zavést</i>
A.5.1.2	Přezkoumání politik pro bezpečnost informací	<i>zavést</i>
A.6	Organizace bezpečnosti informací	
A.6.1	Interní organizace	
A.6.1.1	Role a odpovědnosti bezpečnosti informací	<i>aktualizovat</i>
A.6.1.2	Princip oddělení povinností	<i>zavést</i>
A.6.1.3	Kontakt s příslušnými orgány a autoritami	<i>aktualizovat</i>
A.6.1.4	Kontakt se zájmovými skupinami	<i>ignorovat</i>
A.6.1.5	Bezpečnost informací v řízení projektů	<i>ignorovat</i>
A.6.2	Mobilní zařízení a práce na dálku	
A.6.2.1	Politika mobilních zařízení	<i>zavést</i>
A.6.2.2	Práce na dálku	<i>zavést</i>

A.7	Bezpečnost lidských zdrojů	
A.7.1	Před vznikem pracovního vztahu	
A.7.1.1	Prověřování	<i>zavést</i>
A.7.1.2	Podmínky pracovního vztahu	<i>aktualizovat</i>
A.7.2	Během pracovního vztahu	
A.7.2.1	Odpovědnosti vedení organizace	<i>zavést</i>
A.7.2.2	Povědomí, vzdělávání a školení bezpečnosti informací	<i>zavést</i>
A.7.2.3	Disciplinární řízení	<i>zavést</i>
A.7.3	Ukončení a změna pracovního vztahu	
A.7.3.1	Odpovědnosti při ukončení nebo změně pracovního vztahu	<i>zavést</i>
A.8	Řízení aktiv	
A.8.1	Odpovědnost za aktiva	
A.8.1.1	Seznam aktiv	<i>zavést</i>
A.8.1.2	Vlastnictví aktiv	<i>zavést</i>
A.8.1.3	Přípustné použití aktiv	<i>zavést</i>
A.8.1.4	Navrácení aktiv	<i>zavést</i>
A.8.2	Klasifikace informací	
A.8.2.1	Klasifikace informací	<i>zavést</i>
A.8.2.2	Označování informací	<i>zavést</i>
A.8.2.3	Manipulace s aktivy	<i>zavést</i>
A.8.3	Manipulace s médii	
A.8.3.1	Správa výměnných médií	<i>zavést</i>
A.8.3.2	Likvidace médií	<i>zavést</i>
A.8.3.3	Přeprava fyzických médií	<i>zavést</i>
A.9	Řízení přístupu	
A.9.1	Požadavky organizace na řízení přístupu	
A.9.1.1	Politika řízení přístupu	<i>zavést</i>
A.9.1.2	Přístup k sítím a síťovým službám	<i>zavést</i>
A.9.2	Řízení přístupu uživatelů	
A.9.2.1	Registrace a zrušení registrace uživatele	<i>zavést</i>
A.9.2.2	Správa uživatelských přístupů	<i>ignorovat</i>
A.9.2.3	Správa privilegovaných přístupových práv	<i>ignorovat</i>
A.9.2.4	Správa tajných autentizačních informací uživatelů	<i>ignorovat</i>
A.9.2.5	Přezkoumání přístupových práv uživatelů	<i>ignorovat</i>
A.9.2.6	Odebrání nebo úprava přístupových práv	<i>zavést</i>
A.9.3	Odpovědnosti uživatelů	
A.9.3.1	Používání tajných autentizačních informací	<i>zavést</i>
A.9.4	Řízení přístupu k systémům a aplikacím	
A.9.4.1	Omezení přístupu k informacím	<i>ignorovat</i>
A.9.4.2	Bezpečné postupy přihlášení	<i>ignorovat</i>
A.9.4.3	System správy hesel	<i>zavést</i>
A.9.4.4	Použití privilegovaných programových nástrojů	<i>ignorovat</i>
A.9.4.5	Řízení přístupu ke zdrojovým kódům programů	<i>ignorovat</i>

A.10	Kryptografie	
A.10.1	Kryptografická opatření	
A.10.1.1	Politika pro použití kryptografických opatření	<i>zavést</i>
A.10.1.2	Správa klíčů	<i>zavést</i>
A.11	Fyzická bezpečnost a bezpečnost prostředí	
A.11.1	Bezpečné oblasti	
A.11.1.1	Fyzický bezpečnostní perimetr	<i>zavést</i>
A.11.1.2	Fyzické kontroly vstupu	<i>ignorovat</i>
A.11.1.3	Zabezpečení kanceláří, místností a vybavení	<i>ignorovat</i>
A.11.1.4	Ochrana před vnějšími hrozbami a hrozbami prostředí	<i>zavést</i>
A.11.1.5	Práce v bezpečných oblastech	<i>ignorovat</i>
A.11.1.6	Oblasti pro nakládku a vykládku	<i>ignorovat</i>
A.11.2	Zařízení	
A.11.2.1	Umístění zařízení a jeho ochrana	<i>zavést</i>
A.11.2.2	Podpůrné služby	<i>zavést</i>
A.11.2.3	Bezpečnost kabelových rozvodů	<i>zavedeno</i>
A.11.2.4	Údržba zařízení	<i>zavést</i>
A.11.2.5	Přemístění aktiv	<i>zavést</i>
A.11.2.6	Bezpečnost zařízení a aktiv mimo prostory organizace	<i>zavést</i>
A.11.2.7	Bezpečná likvidace nebo opakované použití zařízení	<i>zavést</i>
A.11.2.8	Uživatelská zařízení bez obsluhy	<i>zavést</i>
A.11.2.9	Zásada prázdného stolu a prázdné obrazovky monitoru	<i>zavést</i>
A.12	Bezpečnost provozu	
A.12.1	Provozní postupy a odpovědnosti	
A.12.1.1	Dokumentované provozní postupy	<i>zavést</i>
A.12.1.2	Řízení změn	<i>zavést</i>
A.12.1.3	Řízení kapacit	<i>zavést</i>
A.12.1.4	Princip oddělení prostředí vývoje, testování a provozu	<i>ignorovat</i>
A.12.2	Ochrana proti malwaru	
A.12.2.1	Opatření proti malwaru	<i>aktualizovat</i>
A.12.3	Zálohování	
A.12.3.1	Zálohování informací	<i>zavést</i>
A.12.4	Zaznamenávání formou logů a monitorování	
A.12.4.1	Zaznamenávání událostí formou logů	<i>ignorovat</i>
A.12.4.2	Ochrana logů	<i>ignorovat</i>
A.12.4.3	Logy o činnosti administrátorů a operátorů	<i>ignorovat</i>
A.12.4.4	Synchronizace hodin	<i>ignorovat</i>
A.12.5	Správa provozního softwaru	
A.12.5.1	Instalace softwaru na provozní systémy	<i>zavést</i>
A.12.6	Řízení technických zranitelností	
A.12.6.1	Řízení technických zranitelností	
A.12.6.2	Omezení instalace softwaru	<i>zavést</i>
A.12.7	Hlediska auditu informačních systémů	

A.12.7.1	Opatření k auditu informačních systémů	<i>ignorovat</i>
A.13	Bezpečnost komunikací	
A.13.1	Správa bezpečnosti sítě	
A.13.1.1	Opatření v sítích	<i>zavést</i>
A.13.1.2	Bezpečnost síťových služeb	<i>zavést</i>
A.13.1.3	Princip oddělení v sítích	<i>zavést</i>
A.13.2	Přenos informací	
A.13.2.1	Politiky a postupu při přenosu informací	<i>zavést</i>
A.13.2.2	Dohody o přenosu informací	<i>zavést</i>
A.13.2.3	Elektronické předávání zpráv	<i>zavést</i>
A.13.2.4	Dohody o utajení nebo o mlčenlivosti	<i>aktualizovat</i>
A.14	Akvizice, vývoj a údržba systémů	
A.14.1	Bezpečnostní požadavky informačních systémů	
A.14.1.1	Analýza a specifikace požadavků bezpečnosti informací	<i>ignorovat</i>
A.14.1.2	Zabezpečení aplikačních služeb ve veřejných sítích	<i>ignorovat</i>
A.14.1.3	Ochrana transakcí aplikačních služeb	<i>ignorovat</i>
A.14.2	Bezpečnost v procesech vývoje a podpory	
A.14.2.1	Politika bezpečného vývoje	<i>ignorovat</i>
A.14.2.2	Postupy řízení změn systémů	<i>ignorovat</i>
A.14.2.3	Technické přezkoumání aplikací po změnách provozní platformy	<i>ignorovat</i>
A.14.2.4	Omezení změn softwarových balíků	<i>ignorovat</i>
A.14.2.5	Principy budování bezpečných systémů	<i>ignorovat</i>
A.14.2.6	Prostředí bezpečného vývoje	<i>ignorovat</i>
A.14.2.7	Outsourcing vývoj	<i>ignorovat</i>
A.14.2.8	Testování bezpečnosti systémů	<i>ignorovat</i>
A.14.2.9	Testování akceptace systémů	<i>ignorovat</i>
A.14.3	Data pro testování	
A.14.3.1	Ochrana dat pro testování	<i>ignorovat</i>
A.15	Dodavatelské vztahy	
A.15.1	Bezpečnost informací v dodavatelských vztazích	
A.15.1.1	Politika bezpečnosti informací pro dodavatelské vztahy	<i>ignorovat</i>
A.15.1.2	Bezpečnostní požadavky v dohodách s dodavateli	<i>ignorovat</i>
A.15.1.3	Dodavatelský řetězec informačních a komunikačních technologií	<i>zavést</i>
A.15.2	Řízení dodávek služeb dodavatelů	
A.15.2.1	Monitorování a přezkoumávání služeb dodavatelů	<i>ignorovat</i>
A.15.2.2	Řízení změn ve službách dodavatelů	<i>ignorovat</i>
A.16	Řízení incidentů bezpečnosti informací	
A.16.1	Řízení incidentů bezpečnosti informací a zlepšování	
A.16.1.1	Odpovědnosti a postupy	<i>aktualizovat</i>
A.16.1.2	Hlášení událostí bezpečnosti informací	<i>zavést</i>
A.16.1.3	Hlášení slabých míst bezpečnosti informací	<i>zavést</i>
A.16.1.4	Posouzení a rozhodnutí o událostech bezpečnosti informací	<i>zavést</i>

A.16.1.5	Reakce na incidenty bezpečnosti informací	<i>zavést</i>
A.16.1.6	Ponaučení z incidentů bezpečnosti informací	<i>zavést</i>
A.16.1.7	Shromažďování důkazů	<i>zavést</i>
A.17	Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací	
A.17.1	Kontinuita bezpečnosti informací	
A.17.1.1	Plánování kontinuity bezpečnosti informací	<i>ignorovat</i>
A.17.1.2	Implementace kontinuity bezpečnosti informací	<i>ignorovat</i>
A.17.1.3	Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací	<i>ignorovat</i>
A.17.2	Redundance	
A.17.2.1	Dostupnost vybavení pro zpracování informací	<i>ignorovat</i>
A.18	Soulad s požadavky	
A.18.1	Soulad s právními a smluvními požadavky	
A.18.1.1	Identifikace odpovídající legislativy a smluvních požadavků	<i>zavést</i>
A.18.1.2	Ochrana duševního vlastnictví	<i>zavést</i>
A.18.1.3	Ochrana záznamů	<i>zavést</i>
A.18.1.4	Soukromí a ochrana osobních údajů	<i>aktualizovat</i>
A.18.1.5	Regulace kryptografických opatření	<i>zavést</i>
A.18.2	Přezkoumání bezpečnosti informací	
A.18.2.1	Nezávislá přezkoumání bezpečnosti informací	<i>ignorovat</i>
A.18.2.2	Shoda s bezpečnostními politikami a normami	<i>ignorovat</i>
A.18.2.3	Přezkoumání technické shody	<i>ignorovat</i>

Tabulka 12 - Vybraná opatření dle normy ISO 27001 (Zdroj upraveno dle [6])

## 3.2 Popis jednotlivých opatření

V této kapitole jsou popsána jednotlivá opatření, které budeme na základě tabulky č. 12, zavádět nebo aktualizovat. Jednotlivá opatření budou snižovat hodnotu rizika a hrozby na akceptovatelnou úroveň. Jelikož se jedná o malou organizaci s málo zaměstnanci, bude velká odpovědnost vytvoření systému řízení bezpečnosti na majitelce organizace.

### 3.2.1 Politiky bezpečnosti informací (A.5)

Cílem opatření je vytvořit politiku bezpečnosti informací, se kterou souhlasí vedení organizace a pravidelně jí přezkoumává z důvodů vhodnosti, přiměřenosti a efektivnosti.

#### Politiky pro bezpečnost informací (A.5.1.1)

Pro zajištění zvyšování bezpečnosti informací v organizaci je nutné vytvořit sadu politik. Tyto politiky budou v souladu s normami, zákony a samotnou politikou organizace. Tuto politiku musí posvětit majitelka organizace a seznámit s touto politikou všechny své

zaměstnance. Seznámení s touto politikou by měli být i klienti společnosti nebo další zainteresované strany. Cílem této politiky je určit, jak bude společnost přistupovat k bezpečnosti informací. Je nutné, aby vedení organizace:

- Definovalo své cíle, směr a oblast jak bude řídit bezpečnost informací
- Definovalo a vysvětlilo jaké pravidla, principy a zásady ohledně bezpečnosti informací
- Definovalo, kdo bude mít jakou odpovědnost a pravomoc při řízení bezpečnosti informací
- Zajistilo neustálé obnovování a zlepšování o znalostech bezpečnosti informací ze strany zaměstnanců a vedení organizace.

V příloze č. 1 je vytvořen návrh takovéto politiky bezpečnosti pro organizaci.

Doba potřebná pro vytvoření těchto politik: 20 hodin.

#### **Přezkoumání politik pro bezpečnost informací (A.5.1.2)**

Každá z vytvořených politik pro bezpečnost informací musí být v pravidelných intervalech přezkoumány, aby byla zajištěna vhodnost, přiměřenost a efektivnost vytvořených politik bezpečnosti. Navrhuji, aby se jednotlivá přezkoumání prováděla jednou za rok nebo pokud nastane výrazná změna v organizace. Provedené přezkoumání musí být opět provedeno odpovědnou osobou, jež bude za danou politiku odpovědný, a každá aktualizovaná politika musí být opět schválena majitelkou společnosti.

Doba nutná pro vytvoření politiky pro přezkoumání bezpečnosti: 10 hodin.

Doba nutná pro přezkoumání: 10 hodin/přezkoumání.

#### **3.2.2 Organizace bezpečnosti informací (A.6)**

Tato opatření mají zajistit bezpečnost informací v organizaci na základě stanovení rámce pro zahájení, implementaci. Opatření musí zabezpečovat bezpečnost informací i při použití mobilních zařízení nebo při práci na dálku.

### **Role a odpovědnosti bezpečnosti informací (A.6.1.1)**

Na základě vytvořených bezpečnostních politik musí být přiděleny odpovědnosti za ochranu jednotlivých aktiv. Odpovědnosti by měly být určeny v oblastech řízení rizik, bezpečnosti informací a za akceptování zbytkového rizika. Jednotlivci s odpovědností za bezpečnost informací mohou své úkoly ohledně bezpečnosti delegovat na další zaměstnance, ale i delegování těchto úkolů za bezpečnost, je nezbujuje jejich odpovědnosti.

Majitelka organizace bude odpovědná za dodržování směrnic ohledně bezpečnosti informací a půjde ostatním zaměstnancům příkladem.

V rámci politiky bezpečnosti informací (příloha č. 1) bude vytvořena pozice nového pracovníka, který bude mít na starost bezpečnosti informací. Tento pracovník bude odpovídat za dodržování směrnic týkající se bezpečnosti informací a dále navrhopat nová opatření snižující hodnotu rizik a zvyšovat ochranu aktiv organizace. Dále bude mít na starost školení zaměstnanců organizace v bezpečnosti informací alespoň jednou ročně. Zaměstnanec bezpečnosti informací bude podřízený pouze majitelce organizace.

Dodržování směrnic bezpečnosti informací bude zaneseno i do pracovních smluv zaměstnanců včetně postihů za jejich nedodržení.

Doba nutná k vytvoření rolí a odpovědností: 12 hodin.

### **Princip oddělení povinností (A.6.1.2)**

Povinnosti a oblasti působení zaměstnanců musí být odděleny, aby se eliminovala možnost pro neoprávněné změny nebo zneužití aktiv organizace. Je důležité, aby neoprávněná osoba nemohla přistupovat, upravovat nebo používat aktiva organizace bez oprávnění nebo bez případné detekce.

Role jednotlivých pracovníků bude rozdělena podle přístupu k aktivům. Takže běžní zaměstnanci nebudou mít přístup bez schválení majitelky do archivu organizace, tam bude mít přístup pouze majitelka a bezpečnostní pracovník po vyzvednutí klíčů od archivu u majitelky. Zaměstnanci nebudou mít přístup ke všem datům klientů organizace, nebudou moci spravovat IT/ICT apod.

Doba nutná k vytvoření oddělených povinností: 8 hodin.

### **Kontakt s příslušnými orgány a autoritami (A.6.1.3)**

V organizaci by se měly zavést směrnice, ve kterých bude popsán postup jak kontaktovat a komunikovat s autoritami (např. orgány vymáhající právo, orgány dohledu). Součástí směrnice by měly být i způsob hlášení identifikovaných bezpečnostních incidentů.

Kontakt s autoritami ohledně bezpečnosti informací je součástí povinností pracovníka bezpečnosti informací. Dále moci kontaktovat IT organizaci v důsledku řešení problémů s bezpečnosti informací.

Ostatní kontakty bude zajišťovat majitelka organizace, která bude jednat za celou svou organizaci s IT společnostmi, orgány vymáhající právo, finančními úřady, klienty, dodavatele elektřiny apod.

Doba na nutná k vytvoření směrnice: 2 hodiny

### **Politika mobilních zařízení (A.6.2.1)**

Jelikož se v organizaci využívají mobilní zařízení tak je nutné vytvořit politiku bezpečnosti pro tuto oblast. Zde je nutné, aby byla zvýšená pozornost ohledně bezpečnosti informací, aby nedocházelo k úniku dat nebo přímo krádeží zařízení na veřejných místech, zasedacích místnostech nebo jiných nechráněných oblastech během využívání mobilních zařízení. Zařízení, která budou obsahovat důležité nebo citlivé informace, jenž souvisí s podnikatelskou činností organizace, nesmí zůstat bez dozoru a jeli to možné tak by měla být uzamčená.

Jestliže bude zaměstnanec vykonávat pracovní činnost, mimo prostory organizace na svém notebooku, nesmí zaměstnanec opustit toto zařízení a nechat jej tak bez dozoru. V případě ztráty důvěrných informací nebo krádež osobního zařízení s důvěrnými firemními informacemi bude proti němu zahájeno disciplinární řízení. Zvláště se toto opatření týká vykonávání práce na veřejném prostranství. V případě práce z domova musí zaměstnanec uzamknout počítač, jestliže opustí počítač, aby ostatní obyvatelé domova, neměli přístup k důvěrným informacím. V případě krádeže mobilního zařízení obsahující důvěrná data informuje o tom pracovníka bezpečnosti informací.

Jelikož majitelka organizace bude pracovat na pracovním notebooku tak musí její pevný disk být šifrován, jelikož obsahuje důvěrné a citlivé údaje organizace. Majitelka je taky odpovědná za používání notebooku mimo kancelář, kde je větší pravděpodobnost krádeže samotného zařízení.

Doba nutná pro vytvoření politiky mobilních zařízení: 5 hodin.

### **Práce na dálku (A.6.2.2)**

Při využití možnosti pracovat mimo kanceláře je nutné vytvořit politiku, která bude definovat podmínky a omezení při práci mimo kanceláře. Je nezbytné zabezpečit komunikaci mezi zařízeními, eliminovat hrozby nebo neautorizovaný přístup k informacím, ochranu před malware a požadavky na firewall a zajišťovat licenční dohody týkající se softwaru. Tyto směrnice by měly zahrnovat fyzickou bezpečnost, pravidla k přístupu návštěvníků k zařízením, audit a monitorování bezpečnosti, poskytování hardwarové, softwarové podpory a údržby.

Návrh jak se budou moci zaměstnanci přistupovat k vnitřní síti mimo kanceláře. Zaměstnancům bude umožněn přístup pomocí VPN, kde se budou muset autentizovat pomocí uživatelského jména a hesla, které dostanou od správce IT po schválení od majitelky. Postup jak se budou moci zaměstnanci připojit, bude popsán v manuálu, který bude vytvořen po instalaci nových zařízení. Následně získá zaměstnanec přístup do podnikové sítě, kde se bude moci přihlásit ke vzdálené ploše a ke svému účtu jako v práci. Takhle přihlášený zaměstnanec získá přístup k informačnímu systému Helios, aby mohl vykonávat práci jemu určenou. Zaměstnanec tímto ale nebude mít přístup k datům, která bude mít uložena na svém stolním počítači. Přístup VPN bude zajišťovat nově pořízený router ZyXEL SBG3500 AnnexB, který umožňuje VPN, ADSL, Wi-Fi a má stavový firewall. Povolení přístupu k bude udělovat autentizační server, který bude pořízen (více v kapitole A.9.1.2).

Návrh směrnice jak pracovat mimo kanceláře je v příloze č. 2.

Doba nutná k vytvoření směrnice a nastavení pro práci na dálku: 12 hodin.

### **3.2.3 Bezpečnost lidských zdrojů (A.7)**

Lidské zdroje patří mezi nejdůležitější aktiva a je nutné zajistit, aby znali a chápali své povinnosti pro, které najímání do organizace. Jednotlivá opatření se vztahují na období před vznikem pracovního poměru, během pracovního poměru a při ukončení nebo změně pracovního poměru mezi zaměstnancem a organizací.

#### **Prověřování (A.7.1.1)**

V souladu se zákonem a etikou by se mělo provádět prověření potencionálních zaměstnanců v organizaci. Prověřování uchazečů o práci by měla odpovídat i jejich případné pozici, kterou budou vykonávat během pracovního poměru.

Získávání informací o uchazečích bude probíhat na základě dokladů totožnosti, výpisu z rejstříku trestů a na internetu. Pokud uchazeč o práci má uvedenou profesní praxi tak bude zkontrolována i ta u jeho posledního zaměstnavatele. Jelikož organizace zpracovává důvěrné informace třetích stran, bude zde kladen velký důraz na důvěryhodnost uchazeče.

Získávání informací nebudou podléhat pouze nově se ucházející zaměstnanci ale také organizace, se kterými budeme spolupracovat. I o těchto organizacích si musíme zjistit informace, než s nimi uzavřeme smluvní vztah. Informace o organizacích budou vyhledávány v obchodním a insolvenčním rejstříku, dále u partnerů se kterými už organizace spolupracuje pomocí získání referencí na danou společnost.

Doba nutná pro vytvoření směrnic na prověřování: 5 hodin

#### **Podmínky pracovního vztahu (A.7.1.2)**

V podmínkách pracovního vztahu mezi zaměstnancem a zaměstnavatelem nebo mezi naší organizací a klientem této organizace se musí uvádět, jaké mají dané strany povinnosti za bezpečnost informací. V pracovní smlouvě zaměstnanec musí být uvedeny, jakou bude mít zaměstnanec roli a odpovědnost na základě bodu A.6.1.1. Jestliže některá ze smluvních stran má přístup k důvěrným informacím, je nutné, aby před získáním přístupu k těmto informacím, byly podepsané dohody o mlčenlivosti. V dohodě o mlčenlivosti musí být uvedeny i případné tresty pokud jedna ze smluvních stran tuto dohodu nebude akceptovat. U zaměstnanec se tento prohřešek bude řešit v rámci disciplinárního řízení.

Pokud by smluvní partner (organizace) porušila tuto dohodu, trestem by bylo uvalení sankce na tuto společnost v krajním případě i ukončení smluvního vztahu.

Doba nutná na vytvoření směrnic pro podmínky pracovního vztahu: 6 hodin

### **Odpovědnosti vedení organizace (A.7.2.1)**

Majitelka organizace musí vyžadovat od všech zaměstnanců dodržování bezpečnosti informací na základě zavedených postupů a politik organizace. Majitelka organizace odpovídá za to, že všichni zaměstnanci budou:

- seznámení o svých rolích a odpovědnostech ohledně bezpečnosti informací před přístupem k důvěrným informacím a přístupem do IS
- mít k dispozici směrnice kde jsou stanovena očekávání na bezpečnost informací a jejich role v organizaci
- motivování k dodržování bezpečnosti informací
- udržovat dovednosti a kvalifikaci, ve kterých budou pravidelně proškolení

Vedení organizace by mělo jít příkladem a dát projevít podporu politiky bezpečnosti informací v podniku. Motivování zaměstnanci způsobují méně incidentů než špatně motivovaný zaměstnanec.

Doba nutná na vytvoření směrnice pro odpovědnost vedení organizace: 4 hodiny

### **Povědomí, vzdělávání a školení bezpečnosti informací (A.7.2.2)**

Všichni zaměstnanci včetně majitelky společnosti se musí pravidelně proškolovat, aby průběžně zvyšovali bezpečnost informací. Vstupní proškolení nově příchozích zaměstnanců bude provádět majitelka společnosti, seznámením se se směrnicemi.

Školení týkající se bezpečnosti informací bude provádět interní/externí osoba odpovědná za bezpečnost informací v organizaci. Organizace umožní bezpečnostnímu pracovníkovi se vzdělávat v oblasti bezpečnosti informací u externích subjektů a aktivně se zajímat o bezpečnost informací. Bezpečnostní pracovník bude následně provádět jednou ročně pravidelná školení za účasti všech zaměstnanců, kde je bude informovat a obnovovat jejich znalosti bezpečnosti informací. Výklad školení musejí být uzpůsobena jazykovým, technickým a technologickým možnostem školících zaměstnanců. Školení se budou

provádět při nástupu do zaměstnání, při změně pracovní pozice a pravidelně alespoň jednou ročně.

Doba nutná na vytvoření směrnice pro vzdělávání bezpečnosti informací: 10 hodin.

Pravidelná školení v oblasti bezpečnosti informací: 10 hodin ročně.

### **Disciplinární řízení (A.7.2.3)**

Během seznamování nových zaměstnanců se směrnicemi a politikami organizace, je nutné seznámit zaměstnance i se směrnicí, ve které budou definovány, jaké budou sankce za porušení bezpečnosti informací v organizaci. Při porušení bezpečnosti informací se bude brát ohled na to, zda to je první přečin zaměstnance nebo již opakovaný, dále se bude zohledňovat i jaký byl dopad porušení bezpečnosti informací na organizaci. Lehké nebo první přestupky budou řešeny slovním napomenutím. U vážných nebo opakovaných přestupků se budou řešit finanční sankcemi nebo ukončením pracovního vztahu. Jestliže zaměstnanec kriticky poškodí společnost, tak je možné řešit odškodnění i právní cestou.

Doba nutná na vytvoření směrnice pro disciplinární řízení: 8 hodin.

### **Odpovědnosti při ukončení nebo změně pracovního vztahu ( A.7.3.1)**

Je nutné, aby při ukončení pracovně smluvního vztahu mezi zaměstnancem a organizací, byly zrušeny jeho přístupová práva k důvěrným informacím společnosti. E-mailová adresa a přidělené telefonní číslo budou přesměrovány na vedoucího pracovníka, který může opět delegovat tyto kontaktní údaje. Zaměstnanec je povinen dodržet dohodu o mlčenlivosti i po odchodu z organizace. Tudíž nesmí zveřejňovat údaje získané během své působnosti v organizaci veřejnosti.

Doba nutná na vytvoření směrnice pro ukončení či změně pracovního vztahu: 8 hodin.

### **3.2.4 Řízení aktiv (A.8)**

Jenom identifikovaná aktiva organizace je možné řídit, proto je důležitá část seznam aktiv, kde aktiva definujeme a dále je nutné určit odpovědnou osobu za dané aktivum. V této kapitole budou určeny směrnice pro odpovědnost za aktiva, klasifikace informací a manipulace médií. Všechny tyto podkapitoly jsou aktiva organizace. Řízení aktiv spadá v rámci celého systému řízení bezpečnosti informací do ustanovení (viz. kap. 1.7.1)

### Seznam aktiv (A.8.1.1)

Organizace by měla identifikovat a následně vytvořit seznam aktiv, který musí být aktuální, přesný a uspořádaný. Jednotlivých aktivum musí být určený vlastník aktiva a jeho klasifikace. Vytvořením seznamu aktiv pomáháme zlepšit efektivitu ochrany bezpečnosti informací. Tyto seznamy mohou být využitelné i pro jiné účely např. při pojištění, ochrana zdraví. V této práci již byl vyhotoven seznam aktiv v kapitole 2.3 Identifikace aktiv při analýze organizace. Seznam aktiv je nutné pravidelně aktualizovat alespoň jednou za rok.

Doba nutná pro vytvoření seznamu aktiv: 5 hodin.

Kontrola seznamu aktiv: 3 hodiny.

### Vlastnictví aktiv (A.8.1.2)

Vlastníkem aktiva může být jednotlivec nebo i entita odpovědná za správu životního cyklu aktiva. Vlastník aktiva je odpovědný, aby daná aktiva byla:

- inventarizována
- náležitě klasifikována a chráněna
- pravidelně přezkoumávaná omezení přístupu k aktivům a jejich klasifikaci na základě platných politik a směrnic
- zajistit správné zacházení pokud je aktivum vymazáno nebo zničeno

Seznam aktiv s přiřazenými vlastníky je zobrazen v tabulce č. 13.

<b>Aktivum</b>	<b>Vlastník</b>
Počítače a notebook	IT firma, majitelka
Server	IT firma
Tiskárny	Majitelka
Kabeláž a aktivní prvek	IT firma
Informační systém	IT firma
Operační systémy	IT firma
O zaměstnancích	Majitelka
Databáze klientů	Majitelka

Zálohy dat	IT firma, majitelka
Fyzické účetní doklady klientů	Majitelka
Elektronické účetní doklady	Majitelka
Pracovní výkazy	Majitelka
Připojení k internetu	Majitelka
Telefonní služby	Majitelka

**Tabulka 13 - Aktiva organizace a jejich vlastníci (Zdroj: [vlastní zpracování])**

Doba nutná pro přiřazení aktiva vlastníkům: 3 hodiny.

Doba nutná pro obnovu či změnu vlastníků: 1 hodina/rok

### **Přípustné použití aktiv (A.8.1.3)**

Vlastník aktiva musí sestavit pravidla jak s daným aktivem zacházet. Tyto pravidla musí být identifikována, implementována a zdokumentována pro zaměstnance mající přístup k informačnímu aktivu případně pro uživatele třetích stran, kteří mají přístup k informačnímu aktivu. Aktiva nesmí být využita pro práci, která nesouvisí s výkonem pracovních povinností. Důvěrné nebo tajné informace by se neměly kopírovat na přenosné médium bez šifrování daného média nebo přenášet po internetu bez zabezpečení.

Doba nutná na vytvoření směrnice pro přípustné použití aktiv: 5 hodin.

### **Navrácení aktiv (A.8.1.4)**

Zaměstnanci, kteří ukončili smluvní vztah se zaměstnavatelem, musí vrátit všechna aktiva organizace, které měli v držení (přístupové kódy, klíče od kanceláře a další). Jestliže zaměstnanec používal své vlastní zařízení k výkonu práce, tak musí všechny nashromážděné informace vydat organizace a trvale vymazat ze svého zařízení. Pokud zaměstnanec vlastní důležité znalosti ohledně důležitých procesů, které probíhají v organizaci a nejsou zatím zdokumentovány, musí je zaměstnanec zdokumentovat a postoupit organizaci.

Doba nutná na vytvoření směrnice pro navrácení aktiv: 2 hodiny.

### **Klasifikace informací (A.8.2.1)**

Jednotlivé aktiva by měly být svými vlastníky, jelikož jsou za aktiva odpovědní, klasifikovány na základě klasifikačního schématu. Klasifikační schéma by mělo jednotné v celé organizaci a musí zahrnovat ustálený způsob pro klasifikaci a kritéria přezkoumání klasifikace. Klasifikace by měla vycházet z analýzy důvěrnosti, integrity a dostupnosti informačního aktiva. Schéma musí být v souladu s politikou řízení přístupu (A.9.1.1). Klasifikační schéma musí odrážet závislost aktiva ohledně jejich citlivosti a kritičnosti pro organizaci. Výsledky klasifikace musí být v průběhu životního cyklu aktiva aktualizovány. V organizaci budou využity čtyři stupně ochrany:

- **Veřejné informace**, jejichž zveřejnění schválilo vedení organizace, nezpůsobují žádné škody
- **Neveřejné informace**, jejichž zveřejnění není schváleno vedením organizace a jejich únik bude mít malý dopad na chod organizace
- **Soukromé údaje** jsou nutno chránit, jak to vyplývá ze zákona č.101/2000 Sb. zákon o osobních údajích
- **Důvěrné informace**, tyto informace vyplývají ze smluvních vztahů mezi obchodními partnery nebo obchodní tajemství organizace, vyzrazení důvěrných informací výrazně poškodí společnost

Doba nutná na vytvoření směrnice pro klasifikaci informací: 8 hodin.

### **Označování informací (A.8.2.2)**

Klasifikované informace je nutné označit, aby bylo jasné, do které kategorie ochrany patří. Aby nedošlo omylem ke zveřejnění důvěrných údajů, musí být označení jednoduché a snadno rozpoznatelné. Označeny musí být jak fyzické tak i elektronické dokumenty. Důvěrné a soukromé údaje musí být opatřeny vodoznakem. Neveřejné a veřejné informace budou mít označení na začátku uprostřed dokumentu. Každý zaměstnanec a obchodní partner musí být seznámen s principem označování dokumentů.

Doba nutná na vytvoření směrnice pro označování informací: 5 hodin.

### **Manipulace s aktivy (A.8.2.3)**

Na základě získané klasifikace informačních aktiv musí být vytvořen postup jak zacházet, zpracovávat, ukládat a předávat informace. Tyto postupy se musí zavést pro jednotlivé úrovně klasifikace a seznámit s nimi zaměstnance. Při manipulaci s důvěrnými a soukromými aktivy je nutné zajistit omezení přístupu k těmto aktivum, to bude zajištěno zamykatelnou skříní v místnosti majitelky organizace.

Doba nutná na vytvoření směrnice pro manipulaci s aktivy: 4 hodiny.

### **Správa výměnných médií (A.8.3.1)**

Ve společnosti se využívají USB flash disky pro přenos informací, proto je nutné vytvořit postupy jak s přenosnými médii pracovat. Tyto postupy by měly zohledňovat:

Jakýkoliv obsah, který uložen na vyměnitelném mediu musí být neobnovitelně odstraněn, pokud už není potřeba

- Při likvidaci přenosného média by měl být vytvořen záznam o takovéto likvidaci
- Uložení média musí odpovídat podmínkám výrobce přenosného zařízení
- Jestliže se budou přenášet důvěrné informace je nutné dané médium šifrovat pomocí kryptografickými techniky
- Pravidelně kontrolovat čitelnost dat na přenosném mediu případně přehrát na nové médium

Doba nutná na vytvoření směrnice pro správu výměnných médií: 3 hodiny.

### **Likvidace médií (A.8.3.2)**

Vytvořením postupů pro permanentní likvidaci médií musí zajistit, že aplikování těchto postupů nebude možné obnovit data, která se nacházela na daném mediu. Způsob likvidace médií bude pomocí skartace nebo neobnovitelný způsob vymazání (např. pomocí spalování). Neobnovitelným vymazáním by se měly likvidovat všechna aktiva bez ohledu na jejich klasifikaci.

Pro kvalitní likvidaci médií bude pořízeno skartovací zařízení Fellowes 53 C, které zvládne i bezpečnou likvidaci DVD nosičů. O skartování médií se vyplní záznam do

tabulky, která bude umístěna u skartovačky. Tabulka bude obsahovat název dokumentu (media), datum skartace a osoba, která skartaci schválila a provedla.

Doba nutná na vytvoření směrnice pro likvidaci médií: 1 hodina.

### **Přeprava fyzických medií (A.8.3.3)**

Média určená k přepravě informačních aktiv musí být chráněna proti neautorizovaným přístupem a případným zneužitím či poškození daného média. Využití kurýrních služeb je vázáno na kvalitu doručení a spolehlivost doručení zásilek. Při posílání médií pomocí kurýrních služeb je nutné zabezpečit, aby se dané médium během přepravy nepoškodilo, to má zajistit dostatek obalového materiálu a pojištění zásilky.

Doba nutná na vytvoření směrnice pro přepravu fyzických medií: 3 hodiny.

### **3.2.5 Řízení přístupu (A.9)**

Účelem řízení přístupu je zajistit, aby k systémům, službám a informacím měli pouze osoby s platným oprávněním využívat tyto informace či vybavení organizace. Vytvořením směrnic pro řízení přístupu má primárně zabránit neoprávněnému vstupu do informačního systému organizace.

#### **Politika řízení přístupů (A.9.1.1)**

Vytvořením politiky řízení přístupu se stanovují pravidla, jakým způsobem se bude přistupovat k informacím. Tuto politiku bude navrhovat každý vlastník aktiva, aby bylo jasně definováno, kdo má právo pracovat s daným aktivem společnosti. Právo zacházet s aktivem může být úplné nebo jen v omezené míře na základě jednotlivých rolí v organizaci případně na přímo na jednotlivé pracovníky. Tato práva jsou vázána na jednotlivé role v organizaci. Přístup k aktivu musí být dán pracovníkovi nebo pracovníkům jen po dobu nezbytnou k výkonu práce poté musí být tato práva opět odebrána.

Při zavádění systému bezpečnosti informací bude v počátku povolen přístup přes mobilní zařízení (notebook), pouze majitelce, která bude využívat pracovní notebook, kde je nainstalovaný aktualizovaný antivirus. A bude mít přístup jak k podnikové síti, tak i ke všem datům v IS a všech klientů, které organizace má.

Pracovník bezpečnosti informací a firma zpracovávající IT/ICT v organizaci bude mít přístup do podnikové sítě a do IS nikoliv však k samotným datům jednotlivých klientů organizace. Dále jim bude umožněn přístup k počítačům a serverům organizace z důvodů jejich správy.

Zaměstnanci budou mít přístup k podnikové síti, jestliže budou využívat firemní počítače, i přístup k IS. Bude jim, ale umožněno zobrazit data pouze těch klientů, které mají za úkol zpracovávat, takže nebudou mít přístup ke všem datům všech klientů organizace.

Zaměstnanci nebo osoby nepracující v organizaci, kteří budou chtít využívat možnost připojení k internetu přes mobilní zařízení (tablet, mobil, notebook) bude umožněno se připojit k WLAN, která umožňuje přístup k internetu nikoliv však k podnikové síti. Na takovém zařízení by měli mít nainstalovaný antivirus.

Doba nutná na vytvoření politiky pro řízení přístupu: 6 hodin.

#### **Přístup k sítím a síťovým službám (A.9.1.2)**

V organizaci je možné se připojovat k síti vzdáleně a pracovat mimo kancelář. Tudíž je nutné v organizaci vytvořit politiku týkající se vzdálenému přístupu k síti. Je nutné stanovit, jaké služby budou touto cestou dostupné a kdo bude mít přístup takto pracovat. Přístupy k síti musí být monitorovány, aby bylo možné zjistit, jestli probíhaly i neautorizované přístupy k síti.

Z důvodů oprávněného přístupu do organizace bude pořízen nový server, který bude sloužit jako autentizační, autentifikační a účtovací (AAA server). Tuto službu bude zajišťovat protokol 802.1x (RADIUS protokol), který bude fungovat na novém serveru. Přihlašovaný uživatel získá přístup k síťovým službám na základě svého jména a hesla. Implementace protokolu RADIUS bude probíhat přes software freeRADIUS. Pokud bude mít uživatel dostatečné oprávnění, dostane přístup pracovat s informačním systémem organizace nebo dostane přístup k internetu nebo nebude připojen. Kvůli zavedení AAA serveru je nutné pořídit i nový switch, který zvládá protokol 802.1x.

Odpovědná osoba: externí IT společnost.

Doba nutná na vytvoření přístupu pro přístup k síti a síťovým službám: 8 hodin.

### **Registrace a zrušení registrace uživatele (A.9.2.1)**

Nový zaměstnanec obdrží od správce systému přihlašovací jméno a heslo, které mu poslouží k přístupu do informačního systému společnosti. Tyto přihlašovací údaje jsou vytvořeny na základě role v organizaci. Jakmile zaměstnanec ukončí svůj pracovní právní vztah s organizací, je důležité, aby administrátor zrušil přihlašovací údaje a heslo daného zaměstnance, aby neměl možnost se neoprávněně přihlásit.

Vypracování návrhu politiky tvorby a správy uživatelských účtů je uvedeno příloze č. 4.

Odpovědná osoba: externí IT společnost

Doba nutná na vytvoření směrnice pro registraci či zrušení registrace uživatele: 2 hodiny.

### **Odebrání nebo úprava přístupových práv (A.9.2.6)**

Změna přístupových práv se provede na základě pokynů majitelky společnosti. Zaměstnanec potřebuje získat přístup k aktivům pro svůj úkol nebo zaměstnanec ukončil svůj úkol a dále nepotřebuje mít přístup k daným aktivům, případně změnil svou pozici ve společnosti a potřebuje zvýšit oprávnění.

Doba nutná na vytvoření směrnice pro odebrání či úpravu přístupových práv: 3 hodiny.

### **Používání tajných autentizačních informací (A.9.3.1)**

Každý uživatel musí nést odpovědnost za ochranu svých tajných autentizačních údajů. Jakékoliv autentizační údaje nesmí být sdíleny s ostatními ani udržovány v písemné podobě. Vznikne-li podezření z kompromitování autentizačních údajů je zaměstnanec povinen si změnit přihlašovací heslo.

Doba nutná na vytvoření směrnice pro používání tajných autentizačních informací: 2 hodiny.

### **Systém správy hesel (A.9.4.3)**

Každý zaměstnanec obdrží od administrátora jednorázové heslo, které si bude muset hned po prvním přihlášení změnit. Autentizační údaje musí udržovat v tajnosti podle A.9.3.1

všichni zaměstnanci. Aby bylo ve společnosti zajištěno, že si zaměstnanci budou vytvářet kvalitní silná hesla, tak heslo musí splňovat:

- Délka 8-10 znaků
- Alespoň jednu číslice
- Alespoň dvě malá a dvě velká písmena
- Alespoň jeden speciální znak, který není číslice nebo písmeno
- Heslo nesmí mít význam jakéhokoliv slova v jakémkoliv jazyce
- Heslo nesmí obsahovat zjistitelné údaje jako telefonní číslo, datum narození, adresu apod.

Zachování bezpečnosti autentizačních údajů je nutné měnit heslo uživatele každého půl roku. A jednotlivá hesla se nesmí opakovat s předchozími.

Doba nutná na vytvoření směrnice pro systém správy hesel: 1 hodina.

### **3.2.6 Kryptografie (A.10)**

Z důvodů ochrany důvěrnosti, integrity a autenticity informací je třeba zavést a zajistit správné využití kryptografických funkcí.

#### **Politika pro použití kryptografických opatření (A.10.1.1)**

Při využívání kryptografických opatření je důležité vytvořit politiku těchto opatření. Zavedením kryptografických opatření chce v organizaci zajistit důvěrnosti, autenticity, nepopíratelnosti a autentizace. V této politice je nutné stanovit, jaké informace se budou šifrovat, k tomu poslouží klasifikace informací. Dále se musí stanovit, jaký šifrovací algoritmus bude k šifrování použit, jaká je správa klíčů. K nastavení kryptografických opatření je vhodné využít specialisty, aby byla zabezpečena bezpečnost informací.

Kryptovat se budou všechny soubory, které budou určeny k vypálení na DVD, kvůli zvýšení ochrany těchto dat. Dále bude šifrovaný externí disk se zálohami. Ke kryptování bude použit šifrovací algoritmus AES-256b. Kryptovaný bude i pracovní notebook majitelky jelikož jsou na něm uloženy osobní údaje zaměstnanců a důvěrné údaje klientů a organizace samotné.

Doba potřebná k vytvoření této politiky: 5 hodin.

### **Správa klíčů (A.10.1.2)**

Tato opatření se soustředí na životní cyklus kryptografických klíčů od jejich vygenerování, ukládání, archivaci, obnovení, distribuci, vyřazení a zlikvidování. Veškeré kryptografické klíče musí být chráněny proti zveřejnění, modifikací nebo ztrátou. Chráněno by mělo být i zařízení, které generuje kryptografické klíče. Dojde-li ke ztrátě kryptografického klíče nebo jeho poškození musí existovat způsob obnovení zašifrovaných informací.

Doba na vypracování směrnic pro správu klíčů: 5 hodin.

### **3.2.7 Fyzická bezpečnost a bezpečnost prostředí (A.11)**

V této podkapitole se budou navrhovat opatření, které budou mít za úkol zajistit, aby se eliminovala možnost neoprávněných fyzických přístupů do organizace a nevzniklo poškození nebo ztráta informací případně zařízení, která jsou nezbytná pro fungování organizace.

#### **Fyzický bezpečnostní perimetr (A.11.1.1)**

Všichni zaměstnanci mají tři klíče. Jeden je od hlavního vstupu do budovy, kde organizace sídlí, druhý klíč je od vstupu do prostoru organizace a třetí je od vstupu do kanceláře, kde zaměstnanec má svůj pracovní stůl s počítačem. Vždy poslední zaměstnanec kanceláře zkontroluje, zda jsou zavřena všechna a zamkne kancelář.

Na hlavních dveřích organizace a na oknech bude nainstalovaný alarm, který musí první zaměstnanec ráno vypnout a poslední zase zapnout. Tím je organizace chráněna v době, kdy není v práci žádný zaměstnanec. Na alarm bude napojen i elektronická čidla na detekci kouře. Alarmový systém bude v případě porušení bezpečnosti informovat majitelku pomocí SMS. Bezpečnostní kód na aktivaci a deaktivaci alarmu bude společný pro všechny zaměstnance.

Do místnosti, kde se nachází server a skříň s důvěrnými informacemi má majitelka organizace. Tento klíč může v případě potřeby propůjčit zaměstnanci.

Každý zaměstnanec má k dispozici stůl, ve kterém se nachází alespoň jedna uzamykatelná zásuvka. Tu je nutné po opuštění pracovní doby zamýkat a ukládat do ní citlivé informace.

Osoby, které vstupují do prostoru organizace, musí zazvonit na zvonek před vstupem a zaměstnance následně dojde otevřít dveře návštěvě. Tímto způsobem je zaručeno, že žádné neoprávněné osoby nebudou bez dohledu zaměstnance.

Alespoň jednou ročně je nutné prověřit funkčnost alarmu včetně stavu baterií. Tuto kontrolu bude provádět spolčenost, která alarm instalovala.

Doba nutná na vytvoření směrnice pro fyzicky bezpečnostní perimetr: 10 hodin.

Doba potřebná na kontrolu zařízení: 2 hodiny/rok.

#### **Ochrana před vnějšími hrozbami a hrozbami prostředí (A.11.1.4)**

Organizace není bezprostředně ohrožena přírodními hrozbami. Na základě protipožární ochrany budovy jsou na každém patře rozmístěny hasicí přístroje. Ochranu proti požáru zajišťuje elektronický požární systém, který je součástí pořizovaného alarmu. Ochranou proti zaplavení se není třeba zabývat, jelikož pravděpodobnost vzniku zaplavení je zanedbatelná.

Ochrana proti neoprávněnému vstupu spočívá v bezpečnostních zámcích na dveřích organizace a kancelářských dveřích a alarmu na vstupních dveřích a oknech organizace.

Doba nutná na vytvoření směrnice pro ochranu před vnějšími hrozbami: 10 hodin.

Doba nutná na ověření funkčnosti kouřových čidel: 2 hodiny/rok.

#### **Umístění zařízení a jeho ochrana (A.11.2.1)**

V organizaci se nachází server, na který se uživatelé přihlašují. Tento server je umístěný v archivu organizace. Klíče od archivu má pouze majitelka organizace. Server a síťové prvky jsou v archivu umístěny na stole, takže se mohou poškodit pádem ze stolu či převržením serveru. Je tedy nutné je proti tomu zabezpečit.

Ostatní zařízení jsou uloženy ve stolech asi 10 cm nad podlahou a tak nehrozí jejich převržení.

Doba nutná na vytvoření směrnice pro umístění zařízení a jeho ochranu: 5 hodin.

#### **Podpůrné služby (A.11.2.2)**

Podpůrné služby se budou týkat pouze zajištění provozu při výpadku elektrické energie. Opatření bude provedeno zakoupením UPS pro každý stolní počítač a server v organizaci, aby bylo možné při výpadku elektrické energie bezpečně uložit a vypnout počítače. Na UPS umístěné u serveru bude připojen modem i switch, tak aby byla zachována po dobu nezbytně nutnou k uložení rozdělané práce, pracovní síť v organizaci.

Do serveru se pořídí druhý HDD a bude zaveden RAID 1 (zrcadlení), aby se minimalizovalo riziko ztráty dat, jestliže bude jeden pevný disk nefunkční. Finanční nároky na zavedení podpůrných služeb je zobrazeno v tabulce č. 16 v ekonomickém zhodnocení.

#### **Údržba zařízení (A.11.2.4)**

Funkčnost serveru a jeho komponent se bude ověřovat externím autorizovaným pracovníkem jednou za rok. Při vzniku jakékoliv poruchy bude neprodleně hlášena odpovědnému pracovníkovi.

Servis tiskárny bude prováděn jednou za půl roku autorizovaných externím pracovníkem nebo při vzniku jakéhokoliv problému. Vzniklé problémy jsou hlášeny vlastníkovi aktiva a ten se musí postarat o rychlou nápravu.

Veškeré revize se musí dokumentovat a probíhat dle pokynů výrobce. Součástí údržby zařízení musí být prověření životnosti baterií u UPS.

Doba nutná na vytvoření směrnice pro údržbu zařízení: 2 hodiny.

Pravidelné kontroly zařízení: 6 hodiny/ rok.

### **Přemístění aktiv (A.11.2.5)**

Přemísťování aktiv, je bez předchozího povolení vedení, je zakázáno. Musí se vytvořit seznam, na kterém bude uvedeno kdo, kdy si půjčil jaké zařízení a kdo mu to povolil a následně uvedeno kdy zařízení nebo aktivum vrátil.

Doba nutná na vytvoření směrnice pro přemístění aktiv: 1 hodina.

### **Bezpečnost zařízení a aktiv mimo prostory organizace (A.11.2.6)**

Bezpečnostní opatření na zařízení, média nebo informační aktiva, která budou vynášena mimo prostory organizace, by mělo být schváleno vedením. Zařízení by neměla zůstat bez dozoru a mít je bezpečně uložena proti poškození, zničení nebo krádeži. Důležité je aby se manipulovalo se zařízeními a aktivy podle pokynů výrobce (nenamáčet zařízení, nevystavovat přímému slunci apod.). Měly by se vést záznamy podle na základě přemísťování aktiv (A.11.2.5).

Doba nutná na vytvoření směrnice pro bezpečnost zařízení a aktiv mimo prostory organizace: 2 hodiny.

### **Bezpečná likvidace nebo opakované použití zařízení (A.11.2.7)**

Kvůli bezpečnému vyřazení médií obsahující důvěrné nebo citlivé údaje zavést postup, jak se budou daná media likvidovat. Likvidace takových to médií musí být permanentní bez jakékoliv možnosti data obnovit. Při likvidaci médií doporučuji data uložená na médiu odstranit a následně i fyzicky zničit dané médium aby bylo navrácení dat na mediu nemožné.

Doba nutná na vytvoření směrnice pro bezpečnou likvidaci: 1 hodina.

### **Uživatelská zařízení bez obsluhy (A.11.2.8)**

Jakmile zaměstnanec ukončí svou pracovní činnost, je důležité, aby vypnul počítač nebo se odhlásil, aby se nikdo bez řádných autentizačních údajů nedostal k informacím, které jsou uloženy na zařízení.

Doba nutná na vytvoření směrnice pro uživatelská zařízení bez obsluhy: 2 hodiny.

### **Zásada prázdného stolu a prázdné obrazovky monitoru (A.11.2.9)**

Cílem tohoto opatření je, aby při ukončení pracovní činnosti zaměstnanec vypnul nebo se odhlásil z počítače (viz A.11.2.8). Ale také, aby papírové dokumenty nebo záznamová média uklidil, nejlépe do uzamykatelného prostoru svého stolu nebo je navrátil na místo, kam patří a nezůstaly ležet volně na stole zaměstnance.

Doba nutná na vytvoření směrnice pro zásadu prázdného stolu a prázdné obrazovky: 2 hodiny.

### **3.2.8 Bezpečnost provozu (A.12)**

Opatření provedené v této kapitole se zaměřují na bezpečný provoz zařízení na zpracování informací v organizaci. Bezpečnost provozu se zajišťuje zavedením provozními postupy, řízením změn a kapacit, nastavením politiky zálohováním nebo jak postupovat při instalaci nového softwaru.

#### **Dokumentované provozní postupy (A.12.1.1)**

Při činnostech, které využívají zařízení pro zpracování informací nebo komunikační zařízení, je nutné vytvořit dokumenty, které budou určovat jak s daným zařízením zacházet. Tyto provozní postupy by se měly vztahovat jak

- Zapnout/vypnout počítač/tiskárnu
- Zálohovat
- Instalovat a konfigurovat nová zařízení
- Instalace a konfigurace nového softwaru
- Zacházet s médii
- Na bezpečnost práce
- Obnovit systém v případě selhání/restartu

Tyto provozní postupy musí schváleny majitelkou organizace a být dostupné pro zaměstnance případě vykonávání těchto činností. Zaměstnanci musí být upozorněni, jestli vznikne nějaká změna v provozních postupech a musí se s ní seznámit.

Doba nutná na vytvoření směrnice pro provozní postupy: 8 hodin.

### **Řízení změn (A.12.1.2)**

Vzniknou-li v organizaci změny v podnikových procesech, vybavení, která zpracovávají informace nebo v systémech zabezpečující bezpečnost informací. Tak tyto změny by měly být řízeny a kontrolovány. Jednotlivé změny musí být naplánované, schváleny majitelkou a testovány ohledně dopadu má změnu na bezpečnosti informací. Všechny změny v podniku by měly mít vedenou dokumentaci s odpovědnosti, nouzovým postupem, odpovědnost za případné přerušení (obnovení) změny. Změny, které jsou pro organizaci prospěšné a splňují požadavky na bezpečnost informací, jsou majitelkou přijaty a jsou upraveny provozní postupy, kterých se změna týká.

Odpovědná osoba: navrhovatel změny a majitelka.

Doba nutná na vytvoření směrnice jak postupovat při řízení změn: 6 hodin.

### **Řízení kapacit (A.12.1.3)**

Na základě řízení kapacit se musí určit, zda máme dostatek lidských zdrojů pro vykonávání naší práce a předejít tak nedostatku lidských zdrojů nebo mít lidských zdrojů přebytek. Další kapacita, kterou je třeba řídit je omezení prostoru pro data na pevných discích počítače. Řešením tohoto problému je vymazat již nepotřebná data nebo pořídit nový pevný disk a zvýšit tak kapacitu diskového pole. Další kapacitu, kterou je třeba také řídit je prostor kanceláří a jejich vybavení. Pokud budeme zaměstnávat mnoho zaměstnanců tak se nám nemusí vejít do stávajících prostor a budeme muset pořizovat nové kanceláře.

Doba nutná na vytvoření směrnice pro řízení kapacit: 2 hodiny.

### **Opatření proti malwaru (A.12.2.1)**

V organizaci je, na všech zařízeních (server, počítače), nainstalovaný antivirový program ESET, který se automaticky aktualizuje. Podniková síť je dále chráněna firewallem, který chrání komunikaci podnikové sítě a internetem a v případě detekování hrozby komunikaci ukončí. Na firewallu je databáze stránek, které mohou být potenciálně nebezpečné.

Při detekování infikování počítače se musí daný počítač zavčas odpojit a zajistit jeho odvirování pomocí antivirového programu. A ručně se vyvolá kontrola všech ostatních počítačů v síti, zda byli taky napadeni nebo ne.

### **Zálohování informací (A.12.3.1)**

Na základě vytvoření směrnice se musí pravidelně vytvářet záložní kopie informací a nastavení systémů. Tyto zálohy musí být v průběhu životnosti zálohy testovány na čitelnost zálohy v případě poruchy. Všichni zaměstnanci pracují s daty, která jsou uložena na serveru.

Návrh pro vytvoření směrnice na zálohování v organizaci je v příloze č. 3.

Doba nutná na vytvoření směrnice pro zálohování: 10 hodin.

### **Instalace softwaru na provozní systémy (A.12.5.1)**

Aktualizace operačního systému, kancelářského softwaru probíhá automaticky po vydání nových aktualizované verze. Oba tyto softwary jsou produkty od společnosti Microsoft. Antivirový program ESET se také aktualizuje s vydáním nové verze. Aktualizace informačního systému, ve které společnost zpracovává účetnictví, bude probíhat jednou za tři měsíce nebo při vydání kritických záplat. Ostatní aktualizace musí probíhat se schválením vedení organizace.

Jestliže bude mít instalovaná aktualizace negativní dopad na chod organizace, měla by být možnost danou aktualizací odstranit. Veškeré instalace na provozní systémy musí být prováděné oprávněným pracovníkem nejlépe externím správcem.

Jednotlivým zaměstnancům není povoleno provádět jakýkoliv změny na provozním systému.

Doba nutná na vytvoření směrnice pro instalaci softwaru na provozní systémy: 2 hodiny.

### **Omezení instalace softwaru (A.12.6.2)**

Zaměstnanci organizace nemají oprávnění instalovat jakýkoliv software na počítače. V případě potřeby instalace nového softwaru je třeba mít povolení od majitelky organizace, která zváží nutnost instalace daného softwaru a jeho dopad na bezpečnost

informací. Omezení instalace je především ochrana jednotlivých IS/ICT v organizaci, aby zaměstnanci nemohli naistalovat nějaký zavírovaný software.

Doba nutná na vytvoření směrnice pro omezení instalace softwaru: 2 hodiny.

### **3.2.9 Bezpečnost komunikací (A.13)**

Účelem zavedení těchto opatření je zabezpečit bezpečnou komunikaci při přenosu informací v sítích a v prostředcích podporující zpracování informací.

#### **Opatření v sítích (A.13.1.1)**

Kontrola a řízení v podnikové síti je odděleno od odpovědnosti zaměstnancům za jejich počítače. Odpovědnost za funkčnost podnikové sítě má externí IT pracovník. Možnost připojit se k podnikové síti musí být omezeno, alespoň autentizací uživatele případně zařízení. Je třeba vypracovat směrnice jak přistupovat k síti, spravovat síťová zařízení.

Odpovědné osoby: majitelka a externí IT pracovník

Doba nutná na aplikaci opatření v síti: 1 hodina.

#### **Bezpečnost síťových služeb (A.13.1.2)**

Při uzavírání smlouvy o síťových službách by měly být ve smlouvě identifikovány a zahrnuty bezpečnostní mechanismy a úroveň poskytovaných služeb. V tomto případě by ve smlouvě měla být stanovena dostupnost přístupu k internetu. V případě nedodržení smluvních podmínek by měla společnost, na základě smluvních podmínek, požadovat odškodnění.

Doba nutná na kontrolu smluvních podmínek síťových služeb: 1 hodina.

#### **Princip oddělení v sítích (A.13.1.3)**

V organizaci je povolené připojení Wi-Fi pro zaměstnance. V organizaci budou zavedeny dvě oddělené sítě VLAN, každá s různými oprávněními. V první síti bude možné na základě autentizace umožněn přístup k informačnímu systému. A v druhé síti bude povolený pouze přístup k internetu.

Odpovědné osoby: majitelka a externí IT pracovník.

Doba nutná na vytvoření směrnice pro princip oddělených sítí: 8 hodin.

### **Politiky a postupu při přenosu informací (A.13.2.1)**

Jelikož komunikace probíhá jak uvnitř organizace, tak i s externími subjekty musí být stanovené směrnice, jak zabezpečit bezpečný přenos informací prostřednictvím všech komunikačních zařízení, aby odeslané informace nedostaly k neoprávněným osobám. Ve směrnici by měla být uvedena opatření proti odposlouchávání, kopírováním, pozměněním nebo zničením informací. Součástí této politiky je i stanovení odpovědnosti v případě vyzrazení nebo ztráty informací. Ve směrnici je třeba poučit zaměstnance, aby neprovozovali důvěrné rozhovory na veřejných místech nebo přes nezabezpečený komunikační kanál. Využíváním e-mailové komunikace při posílání důvěrných informací bude řešeno pomocí kryptografických technik, kvůli ochraně důvěrnosti, integrity a dostupnosti informace.

Doba nutná na vytvoření politik při přenosu informací: 3 hodin.

### **Dohody o přenosu informací (A.13.2.2)**

Dohody mezi organizací a externími stranami musí mít stanoveny dostatečná bezpečnostní opatření pro přenos informací. Tyto dohody mají zabránit ztrátě nebo odcizení informací při přenosu jak elektronických tak i fyzických informací. Bezpečnost přepravy by měla být stanovena podle klasifikace aktiv (A.8.2.1).

Doba nutná na vytvoření dohod o přenosu informací: 2 hodiny.

### **Elektronické předávání zpráv (A.13.2.3)**

Informace zasílané v elektronických zprávách musí být chráněny na základě klasifikačního schématu organizace (A.8.2.1). Během přenosu elektronických zpráv měly by být zajištěny spolehlivost a dostupnost služby, požadavky na elektronický podpis, zajištěna správnost adresování a přeprava zpráv.

Doba nutná na vytvoření směrnice pro elektronické předávání zpráv: 2 hodiny.

#### **Dohody o utajení nebo o mlčenlivosti (A.13.2.4)**

Součástí všech dohod se zaměstnanci nebo externími stranami jsou dohody o mlčenlivosti a o zachování důvěrnosti. Tyto smlouvy se musí pravidelně přezkoumávat a jejich součástí musí být podmínky, které jsou při uplatnění zákonně vymahatelné. Výběr prvků, které budou součástí smlouvy, se volí na základě protistrany a jaký je její přístup k důvěrným informacím případně zacházení s nimi. Při vzniku změny ovlivňující důvěrnost a mlčenlivost se musí smlouvy aktualizovat.

Doba nutná na vytvoření dohod o utajení nebo mlčenlivosti: 2 hodiny.

Doba nutná na kontrolu dohod o utajení nebo mlčenlivosti: 2 hodiny/rok.

#### **3.2.10 Vztahy s dodavateli (15)**

Cílem je zabezpečit všechna aktiva, ke kterým mají přístup externí strany. Při uzavření smlouvy s dodavatelem je nutné stanovit, k jakým aktivům bude mít přístup a manipulovat s danými aktivy.

#### **Řetězec dodavatelů informačních a komunikačních technologií (A.15.1.3)**

V organizaci veškeré služby spojené s IT/ICT zajišťuje externí IT společnost. Je tedy nutné, aby měl dodavatel IC/ICT služeb zaveden systém řízení bezpečnosti informací, jelikož se stará o správu hardwaru, softwaru, podnikovou síť a má přístup k informačním aktivům v organizaci.

Doba nutná kontrola dodavatele IT/ICT: 1 hodina.

#### **3.2.11 Řízení incidentů bezpečnosti informací (A.16)**

Po implementaci těchto opatření pro řízení bezpečnosti informací bude důsledný a efektivní systém bezpečnosti informací při hlášení bezpečnostních událostí a slabých míst.

#### **Odpovědnosti a postupy (A.16.1.1)**

Z aktualizovaných pracovních smluv vyplývá, že jsou všichni zaměstnanci povinni hlásit slabá místa, bezpečnostní události nebo incidenty okamžitě při jejich detekci pracovníkovi bezpečnosti informací. V případě, že pracovník nebude k dispozici, musí

informovat správce IT/ICT nebo majitelku organizace. Povinnost hlásit bezpečnostní události mají i smluvní partneři organizace. Jestliže zaměstnanec neupozorní na tuto situaci, může být podroben disciplinárnímu řízení.

Pracovník bezpečnosti informací zajistí, že po nahlášení incidentu bude incident řádně a co nejrychleji vyhodnocen a vytvořeno účinné opatření a celý proces řádně zdokumentován. A odpovědný za implementaci nových opatření. Jestliže bude řešení finančně nebo časově náročné informuje o tom majitelku organizace.

Doba nutná na vytvoření směrnice pro odpovědnost a postupy: 6 hodin.

### **Hlášení událostí bezpečnosti informací (A.16.1.2)**

Při zjištění bezpečnostní události je zaměstnanec nebo třetí strana je povinen informovat pracovníka bezpečnosti informací. Zaměstnanec vyplní formulář (návrh formuláře v příloze č. 5) a odešle ho na mail nebo odevzdá osobně pracovníkovi bezpečnosti informací. Ve formuláři bude popsán, k jaké bezpečnostní události došlo a jaký to mělo vliv IS nebo dané aktivum organizace. Zaměstnanec musí do formuláře detailně zdokumentovat, co dělal, když vznikla bezpečnostní událost, co se zobrazilo na monitoru a jiné informace, které má v okamžiku vzniku bezpečnostní události k dispozici. Závažná opatření je nutné hlásit osobně nebo telefonicky.

Bezpečnostní události mohou být:

- Neefektivní bezpečnostní opatření
- Lidská chyba
- Politika bezpečnosti informací či jejich směrnice se neshodují
- Překonání fyzické bezpečnosti
- Chyby v softwaru nebo hardwaru
- Narušení důvěrnosti, integrity nebo dostupnosti informací
- Závady indikující útok na bezpečnost.

Pracovník bezpečnosti po vytvoření bezpečnostního opatření Vytvoří záznam o bezpečnostní události a jeho řešení. Zdokumentované bezpečnostní události a jejich opatření uloží do evidence bezpečnosti informací, aby bylo možné jej zpětně dohledat, případně zavést lepší opatření na danou událost. A bylo možné vést záznamy o

bezpečnostních událostech organizace pro efektivnější rozvržení opatření bezpečnosti informací. Jednou měsíčně podá pracovník bezpečnosti informací souhrn nahlášených bezpečnostních událostí majitelce organizace.

Doba nutná na vytvoření hlášení událostí bezpečnosti informací: 4 hodiny.

### **Hlášení slabých míst bezpečnosti informací (A.16.1.3)**

Všechny osoby používající informační systém nebo služeb organizace jsou povinni nahlásit jakákoliv slabá místa bezpečnosti informací. Hlášení musí být podáno co nejrychleji kontaktní osobě, proto musí být způsob hlášení slabých míst jednoduchý a dostupný. Zaměstnanci by neměli zkoušet prokazování slabých míst, jelikož by to mohlo vést k poškození informačního systému nebo by to mohlo být vyhodnocené jako zneužití systému co by vedlo k disciplinárnímu trestu.

Doba nutná na vytvoření směrnice pro hlášení slabých míst: 2 hodiny.

### **Posouzení a rozhodnutí o událostech bezpečnosti informací (A.16.1.4)**

Všechny nahlášené události o slabých místech bezpečnosti na kontaktní místo budou posouzeny odpovědnou osobou. Na základě posouzení události bude následně rozhodnuto, zda bude událost klasifikována jako bezpečnostní incident. Posouzení události je na základně klasifikační stupnice, kterou je třeba stanovit, na základě které se stanoví, jakou prioritu incident má a pomůže tak definovat rozsah a dopad incidentu. Posouzení bezpečnostních událostí se musí zaznamenat, aby byla správnost rozhodnutí ověřena i v budoucnosti.

Doba nutná na vytvoření směrnice a klasifikační stupnice: 3 hodiny.

### **Reakce na incidenty bezpečnosti informací (A.16.1.5)**

Při výskytu bezpečnostního incidentu by měla být reakce kontaktního místa na základě vytvořených postupů. Kontaktní místo musí následně shromáždit důkazy o výskytu bezpečnostního incidentu a co nejdříve obnovit bezpečnost informací na úroveň před výskytem bezpečnostního incidentu. Dále je nutné oznámit vznik bezpečnostního incidentu všem zainteresovaným osobám. Po odstranění incidentu je nutné vše zaznamenat a formálně uzavřít.

Doba nutná na vytvoření směrnice pro reakci na incidenty: 1 hodina.

#### **Ponaučení z incidentů bezpečnosti informací (A.16.1.6)**

Vzniklé bezpečnostní incidenty mohou indikovat potřebu zesílení bezpečnostních opatření, aby se snížil výskyt incidentů, případně se snížili škody způsobené bezpečnostními incidenty. Ponaučení z jednotlivých incidentů lze využít jako reálné příklady při pravidelném školení zaměstnanců.

#### **Shromažďování důkazů (A.16.1.7)**

Je nutné stanovit postupy pro identifikaci, shromažďování, získávání, uchovávání a zacházení s důkazy o incidentech bezpečnosti informací pro účely disciplinárních nebo právních kroků. Tyto postupy by měly zohledňovat bezpečnost důkazů, bezpečnost personálu, kompetence, úlohy a povinnosti zainteresovaných zaměstnanců a dokumentaci.

Doba nutná na vytvoření směrnice pro shromažďování důkazů: 2 hodiny.

### **3.2.12 Soulad s požadavky (A.18)**

Soulad s požadavky má za úkol zabránit vzniku porušování právních nebo smluvních povinností, které jsou vázány na bezpečnost informací nebo jiných požadavků ohledně bezpečnosti. Dále mají tato opatření zabezpečit nezávislé přezkoumání implementace a provoz zavedených politik a směrnic, což souvisí s certifikací ISMS, kterou organizace provádět nebude.

#### **Identifikace odpovídající legislativy a smluvních požadavků (A.18.1.1)**

Stanovením všech požadavků vztahující se na všechny informační systémy a organizaci musí být dle zákona, předpisů a smluvních vztahů identifikovány, dokumentovány a udržovány v aktuálním stavu všechny tyto předpisy.

Doba nutná na identifikaci odpovídající legislativy: 2 hodiny.

#### **Ochrana duševního vlastnictví (A.18.1.2)**

Pro ochranu duševního vlastnictví je nutné stanovit směrnici, která bude zajišťovat soulad s legislativou, předpisy a smluvními požadavky. Mezi produkty spadající do duševního

vlastnictví je software, u kterého je nutné stanovit legální používání softwaru a jiných informačních produktů. Pořizování softwaru musí pouze přes důvěryhodné zdroje, aby se zabezpečilo neporušení autorského práva. Ke každému softwaru musí být stanoveny politiky pro stanovení počtu použitelných licencí, likvidaci softwaru. Licence k používaným softwarům musí být adekvátně uchovány pro případ prokazování platnosti licence. Tato ochrana se nevztahuje pouze na software ale i na dokumenty, manuály, média, knihy apod. Jakékoliv porušení práv duševního vlastnictví musí vést k disciplinárnímu řízení.

Doba nutná na vytvoření směrnic pro ochranu duševního vlastnictví: 2 hodiny.

### **Ochrana záznamů (A.18.1.3)**

Veškeré záznamy v organizaci by měly být chráněny před ztrátou, zničením, falšováním a neoprávněným přístupem. Způsob ochrany záznamů je stanoven klasifikací informací. U jednotlivých záznamů se musí stanovit na jakém médiu a na jak dlouho budou záznamy uloženy. Při využívání paměťových médií je nutné postupovat při ochraně těchto médií podle pokynů výrobce média, aby se předešlo ztrátě dat z důvodů nepřechtení dat z takového média. V průběhu času by se měla zkontrolovat čitelnost dat na těchto médiích a formát souborů, ve kterém byly na médium uloženy.

Doba nutná na vytvoření směrnic pro ochranu záznamů: 4 hodiny.

### **Soukromí a ochrana osobních údajů (A.18.1.4)**

Organizace by měla vypracovat směrnici, která se bude zabývat ochranou soukromí a osobními údaji na základě příslušné legislativy České republiky. Ve směrnici by měla být stanovena odpovědná osoba, která bude zaměstnance poučovat o jejich odpovědnosti s nakládáním osobních informací a zásadami ochrany soukromí.

Doba nutná na vytvoření směrnic pro ochranu osobních údajů: 2 hodiny.

### **Regulace kryptografických opatření (A.18.1.5)**

V souladu s příslušnými dohodami, předpisy a právní legislativou je potřeba stanovit regulaci na použití kryptografických opatření. Je důležité stanovit směrnici, které bude

omezovat použití kryptografických funkcí uvnitř i mimo organizaci. Aby byla dodržena legislativa daného státu, doporučuji vyhledat právní pomoc.

Doba nutná na vytvoření směrnic pro regulaci kryptografických opatření: 4 hodiny.

### **3.3 Postup zavedení změn**

Postup zavedení jednotlivých opatření bude vycházet z potřeb organizace. Tyto potřeby jsou odvozeny z analýzy rizik, která proběhla v kapitole identifikace rizik tabulka č. 11. Kde jsou zobrazeny, která rizika jsou pro organizaci nejvýznamnější a tedy nutné se jimi zabývat co nejdříve.

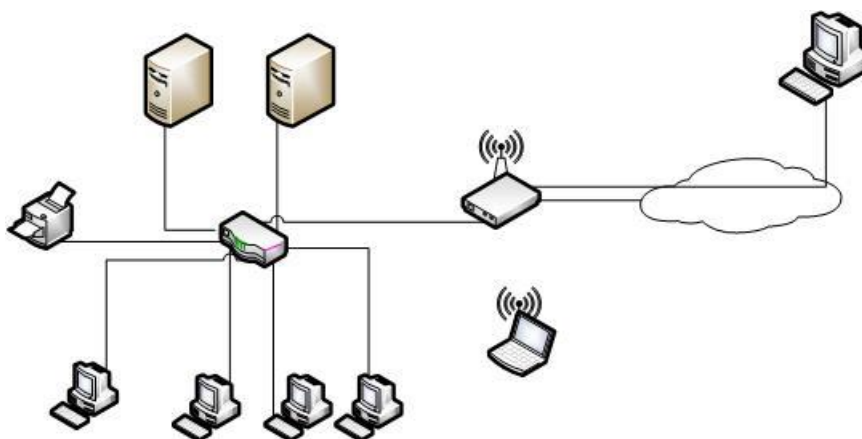
Z analýzy rizik vyplývá, že mezi největší problémy organizace patří dlouhodobější výpadek elektrického proudu, hacknutí počítače nebo serveru a chyby způsobené uživateli a únik přihlašovacích dat. Tyto rizika jsou řešena podle normy ISO/IEC 27002 v kapitolách A.09, A.11 a A.13.

Jako další se budou zavádět opatření z kapitoly A.12. Tato kapitola je spojená se zálohováním informací, které by mělo být uloženo v šifrované podobě tudíž zde bude navazovat i kapitola A.10.

Zaměstnanci podle analýzy rizik jsou pro organizaci velkým rizikem je třeba je vzdělávat v oblasti bezpečnosti informací, než je ale začneme vzdělávat v kapitole A.7 je nutné vytvořit základní politiku bezpečnosti informací v organizaci podle kapitoly A.5 a podle A.6.

Tímto by měla být pokryta největší rizika organizace a jako další se budou postupně zavádět kapitoly A.8, A.16, A.15 a A.18. Kapitoly se budou zavádět v tom pořadí, v jakém jsem je zde uvedl.

Zavedení všech opatření povede k pořízení nových zařízení do organizace, které změní schéma podnikové sítě. Nové schéma je zobrazené na obrázku č.



Obrázek 7 - Nové schéma organizace (Zdroj: vlastní zpracování)

### 3.3.1 Časový plán implementace opatření

Časový harmonogram je sestaven podle postupu zavedení jednotlivých opatření. Implementace systému řízení bezpečnosti informací bude zahájena v 4. 7. 2016. Postup zavádění je znázorněn v tabulce po jednotlivých týdnech.

opatření	Počet hodin	4. 7 - 8. 7	11. 7 - 15. 7	18. 7 - 22. 7	25. 7 - 29. 7	1. 8 - 5. 8	8. 8 - 12. 8	15. 8 - 19. 8	22. 8 - 26. 8	29. 8 - 2. 9
A.5	30									
A.6	42									
A.7	41									
A.8	39									
A.9	22									
A.10	10									
A.11	36									
A.12	30									
A.13	19									
A.15	1									
A.16	18									
A.18	12									

Tabulka 14 - Časový harmonogram (zdroj: vlastní zpracování)

Plánované dokončení implementace všech uvedených opatření bude na konci druhého měsíce implementace tedy koncem srpna 2016.

### 3.4 Ekonomické zhodnocení

V tabulce č. 14 je zobrazen souhrn časové náročnosti na jednotlivé kapitoly z normy ISO/IEC 27001. Celková časová náročnost na zavedení systému řízení bezpečnosti informací je 300 hodin, při předpokládané hodinové mzdě 250 Kč jsou náklady 75 000

Kč. Systém řízení bezpečnosti informací se musí každoročně obnovovat. Je potřeba si na kontrolu ISMS vyhradit každý rok 36 hodin což dělá za rok 9 000 Kč.

Označení	Opatření	Počáteční časová náročnost [hodiny]	Roční kontroly [hodiny]	Počáteční náklady [Kč]	Každoroční náklady [Kč]
A.5	Politiky bezpečnosti informací	30	10	7 500	2 500
A.6	Organizace bezpečnosti informací	42	0	10 500	0
A.7	Bezpečnost lidských zdrojů	41	10	10 250	2 500
A.8	Řízení aktiv	39	4	9 750	1 000
A.9	Řízení přístupu	22	0	5 500	0
A.10	Kryptografie	10	0	2 500	0
A.11	Fyzická bezpečnost a bezpečnost prostředí	36	10	9 000	2500
A.12	Bezpečnost provozu	30	0	7 500	0
A.13	Bezpečnost komunikací	19	2	4 750	500
A.14	Akvizice, vývoj a údržba systémů	0	0	0	0
A.15	Dodavatelské vztahy	1	0	250	0
A.16	Řízení incidentů bezpečnosti informací	18	0	4 500	0
A.17	Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací	0	0	0	0
A.18	Soulad s požadavky	12	0	3 000	0
	Celkem	300	36	75 000	9000

**Tabulka 15 - Náklady na časové vypracování opatření (Zdroj: vlastní zpracování)**

Náklady na vypracování směrnic pro řízení bezpečnosti informací nejsou jediné. Je nutné taky pořídit zařízení nebo media, která budou daná rizika snižovat. Náklady na pořízení jednotlivých materiálních položek pro zajištění bezpečnosti informací v organizaci jsou uvedena v tabulce č. 15, kde jsou i zobrazeny celkové náklady na zavedení ISMS. Náklady na pořízení nových zařízení či medií jsou 54 729 Kč. Ceny v tabulce č. 15 jsou uvedeny bez DPH.

opatření	položka	cena	množství	celkem
A.8.3.2	Fellowes 53 C	2 487,00	1	2 487,00
A.9.1.2	CISCO SLM2008T-EU	2 481,00	1	2 481,00
A.6.2.2	ZyXEL SBG3500 AnnexB	6 786,00	1	6 786,00
A.9.1.2	Dell PowerEdge T20	11 401,00	1	11 401,00
A.11.1.1	Drátový zabezpečovací set s GSM komunikátorem	11 348,00	1	11 348,00
A.11.2.2	APC Back-UPS CS 350I	2 223,00	6	13 338,00
A.11.2.2	WD SE Raid Edition 1TB	1 956,00	1	1 956,00
A.12.3.1	WD 2.5" My Passport Ultra 1TB	1 587,00	1	1 587,00
A.12.3.1	Kingston DataTraveler 2000 16GB	2 412,00	1	2 412,00

A.12.3.1	Verbatim DVD-R Archival 25ks	933,00	1	933,00
Celkem				54 729,00
Zavedení ISMS		250,00	300	75 000,00
Celkem				129 729,00

**Tabulka 16 - Souhrn všech nákladů na zavedení ISMS (Zdroj: vlastní zpracování)**

Zavedení systému řízení bezpečnosti informací v organizaci bude trvat 300 hodin a celkové náklady na zavedení dosáhnou částky 129 729 Kč.

## ZÁVĚR

Tato diplomová práce je rozdělena na tři části teoretická východiska, analýza současného stavu a návrh řešení. V teoretické části jsem se zabýval vysvětlením základních pojmů využívaných v bezpečnosti informací, dále jsem popsal základní normy a zákony, které se zabývají bezpečnosti informací. A popsal postup zavedení systému řízení bezpečnosti informací.

V další části proběhla analýza společnosti. Jaký je její současný přístup k bezpečnosti informací. Současně proběhla analýza aktiv a rizik, která momentálně působí v organizaci. Analýza aktiv a rizik umožnila vzniku matice zranitelnosti, která zobrazuje, jaké rizika jsou v organizaci nejvýznamnější a na která aktiva působí. Tato matice definovala postup zavedení jednotlivých opatření, která jsem ve třetí části této práce navrhl.

V návrhové části jsem na základě přílohy A v normě ISO/IEC 27001:2014 a ISO/IEC 27002:2014 jsem stanovil, která opatření jsou nutná pro zvýšení bezpečnosti informací v organizaci a tím snížit bezpečnostní rizika organizace. Většina opatření týkající se bezpečnosti informací je spojena s vytvořením bezpečnostních směrnic či politik, ale na základě požadavků organizace pro vzdálený přístup se musely pořizovat i nová zařízení, která budou zabezpečovat bezpečné připojení k podnikové síti.

Mezi hlavní bezpečnostní opatření navržená v této práci patří fyzická bezpečnost organizace implementováním elektronického alarmu s požární ochranou, zajištění autentizovaného přístupu mobilních zařízení do organizace, umožnění práce na dálku pomocí VPN a stanovení pravidel pro zálohování. V návrhové části je zahrnuto i ekonomické zhodnocení na zavedení systému řízení bezpečnosti informací. Finanční náklady za zavedení ISMS dosáhly částky 129 729 Kč k tomu roční náklady na přezkoumání a aktualizace těchto zavedení vyjde na 9 000 Kč. Délka trvání zavedení ISMS v organizaci by měla podle plánu trvat 9 týdnů.

Ačkoliv zatím majitelka neplánuje provést certifikaci, která by zvýšila důvěryhodnost organizace před novými, ale i stávajícími klienty. Tato práce pro organizaci poskytuje výhodu už samotnou analýzou aktiv a rizik, na základě, kterých je možné zavést navržená

opatření a tím zvýšit bezpečnost informací v organizaci. Jelikož v ní byly identifikovány bezpečnostní mezery, které byly odstraněny.

## SEZNAM POUŽITÉ LITERATURY

- [1] DOUCEK, Petr. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8
- [2] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Vyd. 1. Brno: Akademické nakladatelství CERM, 2013, 377 s. ISBN 978-80-7204-872-4.
- [3] DOUCEK, Petr, Miloš MARYŠKA a Lea NEDOMOVÁ. Informační management v informační společnosti. 1. vyd. Praha: Professional Publishing, 2013, 264 s. ISBN 978-80-7431-097-3.
- [4] ČSN ISO/IEC 27003. Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Směrnice pro implementaci systému řízení bezpečnosti informací. Praha: Český normalizační institut, 2014
- [5] ČSN ISO/IEC 27000. Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Přehled a slovník. Praha: Český normalizační institut, 2014
- [6] ČSN ISO/IEC 27001. Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. Praha: Český normalizační institut, 2014
- [7] *Ministerstvo vnitra České republiky* [online]. [cit. 2016-04-22]. Dostupné z: <http://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx>
- [8] *Zákon o archivnictví a spisové službě č. 499/2004 Sb.: účinnost od 1. ledna 2005.* Český Těšín: Poradce, 2005. Zákony do kapsy. ISBN 80-736-5055-X.
- [9] NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář.* Vyd. 1. Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-665-5.
- [10] ČSN ISO/IEC 27002. Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací – Požadavky. Praha: Český normalizační institut, 2014
- [11] *Zákon o kybernetické bezpečnosti* [online]. [cit. 2016-05-02]. Dostupné z: [http://www.bureauveritas.cz/wps/wcm/connect/bv\\_cz/local/home/news/press-releases/zakon-o-kyberneticke-bezpecnosti](http://www.bureauveritas.cz/wps/wcm/connect/bv_cz/local/home/news/press-releases/zakon-o-kyberneticke-bezpecnosti)
- [12] *Zákon o kybernetické bezpečnosti v praxi* [online]. [cit. 2016-05-02]. Dostupné z: <http://www.systemonline.cz/it-security/zakon-o-kyberneticke-bezpecnosti-v-praxi.htm>

[13] Kdo a co bude spadat pod nový zákon o kybernetické bezpečnosti [online]. [cit. 2016-05-02]. Dostupné z: <http://www.lupa.cz/clanky/kdo-a-co-bude-spadat-pod-novy-zakon-o-kyberneticke-bezpecnosti/>

[14] ČESKÁ REPUBLIKA. Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. In Sběrka zákonů ČR, ročník 2014, částka 127. [cit. 2016-05-02]. ISSN 1211-1244 Dostupné z: <http://www.zakonyprolidi.cz/cs/2014-317>

[15] ČESKÁ REPUBLIKA. Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. In Sběrka zákonů ČR, ročník 2010, částka 149. [cit. 2016-05-02]. ISSN 1211-1244 Dostupné z: <http://www.zakonyprolidi.cz/cs/2010-432>

[16] ČESKÁ REPUBLIKA. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In Sběrka zákonů ČR, ročník 2014, částka 75. [cit. 2016-05-02]. ISSN 1211-1244 Dostupné z: <http://www.zakonyprolidi.cz/cs/2014-181>

## SEZNAM OBRÁZKŮ

Obrázek 1 - Vzájemné vztahy bezpečnosti informací v organizaci.....	12
Obrázek 2 - Přiměřená bezpečnost za akceptovatelné náklady .....	13
Obrázek 3 - Model PDCA aplikovaný na ISMS.....	14
Obrázek 4 - Vazby mezi normami ISMS .....	20
Obrázek 5 - Řízení rizik.....	23
Obrázek 6 - Schéma podnikové sítě .....	34
Obrázek 7 - Nové schéma organizace.....	77

## SEZNAM TABULEK

Tabulka 1 - Kategorie opatření ISO/IEC 27002 .....	21
Tabulka 2 - Hodnocení aktiv .....	28
Tabulka 3 - Identifikace aktiv .....	35
Tabulka 4 - Klasifikace aktiv v organizaci .....	36
Tabulka 5 - Ohodnocení aktiv firmy.....	37
Tabulka 6 - Pravděpodobnostní klasifikace hrozeb .....	37
Tabulka 7 - Pravděpodobnost vzniku hrozeb .....	38
Tabulka 8 - Hodnocení rizik .....	38
Tabulka 9 - Matice zranitelnosti .....	39
Tabulka 10 - Klasifikace rizik .....	40
Tabulka 11 - Matice rizik.....	41
Tabulka 12 - Vybraná opatření dle normy ISO 27001 .....	46
Tabulka 13 - Časový harmonogram.....	77
Tabulka 14 - Náklady na časové vypracování opatření .....	78
Tabulka 15 - Souhrn všech nákladů na zavedení ISMS .....	79

## **SEZNAM PŘÍLOH**

Příloha č. 1 - Návrh politiky bezpečnosti informací organizace.....	1
Příloha č. 2 - Vypracování směrnic pro práci na dálku .....	1
Příloha č. 3 - Návrh směrnice pro zálohování dat v organizaci.....	1
Příloha č. 4 – Směrnice správy uživatelských účtů .....	1
Příloha č. 5 – Návrh formuláře pro hlášení bezpečnostních událostí v organizaci.....	1

# **Příloha č. 1 - Návrh politiky bezpečnosti informací organizace**

## **Bezpečnostní politika organizace**

### **Cíl bezpečnosti informací**

Bezpečnostní politika si klade za cíl, zajistit dostatečnou ochranu informací a zamezit neautorizovanému přístupu k informacím a jakkoliv s nimi manipulovat.

### **Pravidla bezpečnosti politiky**

- Organizace se zaručuje, že bude zajišťovat bezpečnost informací a jejich ochranu na základě zákonných požadavků České republiky a Evropské unie.
- Organizace se zavazuje, že vytvoří účinný a spolehlivý systém řízení bezpečnosti informací, který bude zajišťovat přiměřenou ochranu informačních aktiv před existujícími bezpečnostními riziky.
- Systém řízení bezpečnosti informací je neoddelitelnou součástí řídicích procesů organizace s hlavním cílem minimalizace rizika nebo jeho odstranění tak aby nedošlo k narušení důvěrnosti, integrity a dostupnosti informací.
- Systém řízení bezpečnosti informací je v organizaci budován podle platných norem ISO/IEC 27 001 a ISO/IEC 27 002.
- Základem řízení bezpečnosti politiky v organizaci je dokument Politika bezpečnosti informací, ve kterém jsou uvedeny pravidla pro systematický přístup ke zvládnutí bezpečnostních rizik.
- Majitelka organizace je nejvyšší rozhodující orgán, který schvaluje systém řízení bezpečnosti informací v organizaci a je odpovědná za dodržování pravidel bezpečnosti informací v celé organizaci.
- Vytvoření interní nebo externí pozice, která se bude zabývat bezpečností informací v organizaci. Pracovník bezpečnosti informací bude mít na starost evidování a řešení bezpečnostních incidentů, sleduje účinnost provozování systému řízení bezpečnosti informací pomocí ročních kontrol. Dbá na dodržování politiky bezpečnosti informací.
- Zaměstnanci jsou povinni dodržovat pravidla bezpečnosti informací, která jsou uvedena v Politice bezpečnosti organizace a dalších směrnících týkajících se

bezpečnosti informací. Jakékoliv změny od definovaných pravidel jsou zaměstnanci povinni hlásit majitelce organizace.

*Místo a den podpisu politiky*

*Podpis majitelky*

## **Příloha č. 2 - Vypracování směrnic pro práci na dálku**

### **Zabezpečení přístupu na dálku do organizace**

Účel: Pokyny k bezpečnému přístupu uživatele k podnikové síti mimo prostor organizace

- Zaměstnanec, po schválení práce na dálku majitelkou organizace, kontaktuje správce sítě, který mu umožní pracovat na dálku prostřednictvím VPN.
- Zaměstnanec musí mít aktualizovaný OS a nainstalovaný antivirus.
- Zaměstnanec pracující mimo kanceláře bude mít stejná oprávnění, jako kdyby vykonával svou práci v prostorách organizace.
- Autentizace přihlašované osoby bude na základě uživatelského jména a hesla, které obdrží od správce sítě během 5 pracovních dní od zažádání o vzdálený přístup.
- Zaměstnanec musí dodržovat pravidla bezpečnosti informací jako by byl v kanceláři.
- Zaměstnanec musí zajistit fyzickou bezpečnost informací a zařízení, která k tomu využívá.
- Postup jak se připojit do organizace bude vydán žadateli správcem sítě nebo majitelkou organizace. V případě potřeby se bude zaměstnanec informovat u správce sítě.
- Zaměstnanec se musí odhlásit od svého účtu v organizaci a od VPN, jakmile dokončí výkon práce.

*Místo a den podpisu politiky*

*Podpis majitelky*

## **Příloha č. 3 - Návrh směrnice pro zálohování dat v organizaci**

### **Stanovení postupu při zálohování dat organizace**

Odpovědná osoba: externí IT společnost

Cíl směrnice: Stanovení postupu při zálohování dat ze serveru a osobních počítačů

Za proces zálohování odpovídá a provádí bezpečnostní pracovník organizace. Dále odpovídá za čitelnost dat na mediích

Postup zálohování serveru:

- Bitové kopie systému se bude zálohovat jednou za 3 měsíce na externí disk.
- Na začátku měsíčně se budou vytvářet úplné zálohy informačního systému na externí disk a vypálí na DVD. Zálohování se bude provádět přes integrovanou funkci Windows Server Backup.
- Každý týden budou vytvořeny přírůstkové zálohy na USB disk, který má heslo na ochranu přístupu k datům.
- Systém okamžité zálohy je řešen nastavením RAID 1 (zrcadlení) na pevném disku serveru.

Postup zálohování počítačů/notebooku:

- Jednou ročně se vytvoří bitové kopie všech počítačů, ty pak budou vypáleny na DVD.
- Každý měsíc se budou vytvářet zálohy důležitých souborů na externí disk. Tyto soubory budou každé 3 měsíce vypáleny na DVD.

Kontrola funkčnosti

- Kontrola čitelnosti záloh bude provedena na DVD discích hned po vypálení a následně každých 6 měsíců.
- Kontrola dat na ostatních médiích se bude provádět vždy po nahrání souboru na medium.

Výběr důležitých dokumentů probíhá na základě klasifikace informací a stanovených provozních postupů organizace.

Uložení záloh bude v kanceláři majitelky po dobu 3 let, následně budou bezpečně likvidovány.

*Místo a den podpisu politiky*

*Podpis majitelky*

## **Příloha č. 4 – Směrnice správy uživatelských účtů**

### **Provozní řád správy uživatelských účtů a jejich přístup k IT/ICT organizace**

Cíl: Vytvoření pravidel zabezpečující přístup uživatele k manipulaci s IT/ICT organizace.

#### Vytvoření uživatelského účtu

- Uživatelské jméno bude vytvořeno prvním písmenem křestního jména a celým příjmením bez diakritiky. Jestliže bude více jmen se stejným uživatelským jménem, bude nakonec přidána číslice (např. Josef Krčmář bude mít uživatelské jméno JKrcmar).
- Nového uživatele vytvoří správce systému (IT společnost) a budou mu přidělena práva podle působnosti v organizaci.
- Správce systému má 5 pracovních dní na vytvoření nového uživatelského účtu od podání žádosti majitelkou organizace.
- Seznámení uživatele s jeho právy, povinnosti a tresty za jejich porušení.

#### Povinnosti uživatele

- Dodržovat směrnice o týkající se bezpečnosti informací
- Informovat správce systému v případě podezření na slabé místo v zabezpečení
- Udržovat své autentizační údaje v tajnosti
- Pravidelně měnit heslo alespoň jednou za půl roku. Heslo musí mít 8-10 znaků (1 číslice, 2 malá a 2 velká písmena, 1 speciální znak)
- Odhlašovat se při opuštění pracovního místa z počítače.

#### Je zakázáno

- Instalovat jakýkoliv software
- Úmyslně porušovat bezpečnost informací
- Ukládat autentizační údaje do programů na správu hesel
- Provádět činnosti porušující autorská a licenční práva
- Jakkoliv manipulovat se sítíovou infrastrukturou organizace
- Pokoušet se připojovat neautorizované zařízení

- Stahování spustitelných programů nebo příloh e-mailu (souboru s příponou \*.exe, \*.com, \*.bat).

#### Zrušení uživatele nebo jeho modifikace

- Změna oprávnění přístupu k informacím, bude provedena na základě konzultace s majitelkou organizace.
- Při zapomenutí hesla bude informován správce systému, který odešle nové přístupové heslo na email zaměstnance.
- Na jeho vlastní žádost
- Ukončením pracovního poměru
- Zrušení či změnu oprávnění provede správce systému

#### Postihy

Postihy jsou zvažovány dle závažnosti a četnosti. Od napomenutí, finanční pokutu až po ukončení pracovního poměru.

*Místo a den podpisu politiky*

*Podpis majitelky*

## Příloha č. 5 – Návrh formuláře pro hlášení bezpečnostních událostí v organizaci

### Formulář pro hlášení bezpečnostních událostí

Formulář hlášení bezpečnostní událostí č. (vyplní bezp. Pracovník)	
Datum	<i>Vyplní zaměstnanec</i>
Čas	<i>Vyplní zaměstnanec</i>
Oznamovatel	<i>Vyplní zaměstnanec</i>
Popis bezpečnostního události	<i>Vyplní zaměstnanec</i>
Popis IS při události	<i>Vyplní zaměstnanec</i>
Podpis oznamovatele	<i>Vyplní zaměstnanec</i>
Kontakt na bezpečnostního pracovníka	JKrcmar@firma.cz
Datum přijetí hlášení	<i>Bezpečnostní pracovník</i>
Čas přijetí hlášení	<i>Bezpečnostní pracovník</i>
ID vypracovaného opatření	<i>Bezpečnostní pracovník</i>
Podpis přijetí bezpeč. pracovníkem	<i>Bezpečnostní pracovník</i>