VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH ZAVEDENÍ NUTNÝCH OBLASTÍ ISMS VE VEŘEJNÉ SPRÁVĚ

THE PROPOSAL FOR IMPLEMENTATION OF ESSENTIAL ISMS SECTIONS AT THE PUBLIC ADMINISTRATION

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Roman Klepárník**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**
SUPERVISOR

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Roman Klepárník**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2017/18

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Návrh zavedení nutných oblastí ISMS ve veřejné správě

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska
Analýza současného stavu
Vlastní návrh řešení
Zhodnocení a přínosy práce
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Pro vybranou organizaci (obec) na základě analýzy, odhalit největší slabiny v oblasti informační bezpečnosti a následně vytvořit sbírku doporučení dle ISMS, která povede ke zvýšení informační bezpečnosti a celkového bezpečnostního povědomí mezi zaměstnanci.

Základní literární prameny:

ČSN ISO/IEC 27001. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27002. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Soubor postupů. Praha: Český normalizační institut, 2014.

ONDRÁK Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-872-4.

Ochrana osobních údajů: zákon o ochraně osobních údajů a další právní předpisy. GDPR - obecné nařízení Evropského parlamentu a rady (EU) 2016/679 o ochraně osobních údajů: redakční uzávěrka 28. 8. 2017. Ostrava: Sagit, 2017. ISBN 978-80-7488-241-8.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2017/18

V Brně dne 28.2.2018

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

ABSTRAKT

Tato diplomová práce se zaměřuje na uplatnění systému řízení bezpečnosti informací ve veřejné správě. Práce se zabývá analýzou nejčastějších hrozeb na informační bezpečnost a popisuje doporučené postupy v souladu s normami řady ISO/IEC 27000. Obsahuje návrh bezpečnostních doporučení, která pomohou organizaci zajistit lepší informační bezpečnost a v přípravě na GDPR.

ABSTRACT

This diploma thesis focuses on the application of information security management system in the public administration. Thesis focuses on the most frequent threats on information security and describes the best practices which are compliant with the ISO/IEC 27000. It contains the proposal of security recommendation that will help the organisation with ensuring better information security and with the preparation for GDPR.

KLÍČOVÁ SLOVA

Obec, normy řady ISO/IEC 27000, obecné nařízení o ochraně osobních údajů, riziko, bezpečnost informací, bezpečnost organizace.

KEYWORDS

Municipality, standards of ISO/IEC 27000, General Data Protection Regulation, risk, information security, organization security.

BIBLIOGRAFICKÁ CITACE

Klepárník, R. *Návrh zavedení nutných oblastí ISMS ve veřejné správě*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2018. 131 s. Vedoucí diplomové práce Ing. Petr Sedlák.

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že předložená 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 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 16. května 2018

……

Podpis studenta

PODĚKOVÁNÍ

Zde bych rád poděkoval svému vedoucímu práce Ing. Petru Sedlákovi za odborné vedení a užitečné rady při vytváření této práce. Dále bych rád poděkoval všem příbuzným, kteří mně byli při tvorbě práce nápomocni.

OBSAH

ÚVOD

Doba jde neustále dopředu a s ní i vývoj informačních technologií. V dnešním světě jsou nejdůležitějším aspektem všech firem, společností, podniků a různých organizací data a informace. Právě informační bezpečnost je u mnoha firem podceňována a opomíjena. Proto je třeba, aby se bezpečnost řešila i ve společnostech, které nejsou technologicky zaměřené, a komunikační a informační technologie využívají pouze jako podpůrný nástroj pro ulehčení pracovních procesů. Protože i tyto společnosti potřebují mít svá data v bezpečí. Je velké množství hrozeb, které mohou na informace a data působit, a stále vznikají nové. Hrozbami už nejsou ovlivňovány pouze pracovní stanice, ale například i přenosná média, zálohovací média, chytré telefony atd. Z toho důvodu je třeba pokrýt nejenom vlastní výpočetní techniku, ale i fyzickou ochranu budov, personálu a hlavně neustále vyhledávat možná rizika působící na společnost a její okolí. Zde je možné využít postupů, které byly postupem času ověřeny a zaváděny ve formě managementu informační bezpečnosti. Management informační bezpečnosti se zabývá ochranou informací a dat v podniku a je popsán mezinárodním souborem norem ISO/IEC 27000. Soubor norem poskytuje doporučení pro ochranu informačních aktiv společnosti. Jedná se o nikdy nekončící proces, ve kterém je neustále monitorován a zlepšován aktuální stav.

V této práci se nejdříve zabývám identifikací hrozeb na aktiva organizace veřejné správy a následně navrhuji soubor opatření na identifikované hrozby. V první části práce jsou představená teoretická východiska (Kapitola 2), která jsou důležitá pro pochopení dalších částí práce. Druhá část je věnována analýze současného stavu bezpečnosti informací v organizaci a analýze rizik (Kapitola 3). Ve třetí části jsou z předešlé analýzy navrženy opatření pro odstranění nebo zmírnění hrozeb (Kapitola 4). Dále jsem vytvořil časový plán opatření, ekonomické zhodnocení a na závěr srovnání, jak organizaci pomůže zavedení opatření dle norem ISO/IEC 27001 a 27002 v přípravě na Obecné nařízení o ochraně osobních údajů.

1 VYMEZENÍ PROBLÉMU A CÍLE PRÁCE

Cílem této diplomové práce je analyzovat současný stav informační bezpečnosti vybrané organizace (obce) a na jeho základě vytvořit soubor doporučení pro eliminaci nebo redukci zjištěných hrozeb s využitím řady norem ISO/IEC 27000. Vedení organizace se tak rozhodlo z důvodu zvýšení bezpečnosti informací a z důvodu přípravy na Obecné nařízení o ochraně osobních údajů. V práci bude popsána první etapa zavádění systému řízení bezpečnosti informací, která poslouží jako předloha pro další etapu a bude vypracován časový harmonogram pro zavedení jednotlivých opatření.

2 TEORETICKÁ VÝCHODISKA

V této části práce jsou vysvětlena teoretická východiska práce, která slouží pro pochopení pojmů spojených s bezpečností informací a zaváděním systému řízení bezpečnosti informací (dále jen ISMS).

2.1 Základní pojmy

Na začátek je nutné seznámit se s pojmy a názvoslovím, které jsou obsaženy v oblasti bezpečnosti informací a které je potřeba znát pro pochopení problematiky práce.

Data

Jde o získané a zachycené údaje popisující realitu. Mohou být získávána například pozorováním, měřením nebo výpočtem. Data existují a jsou uložena na různých médiích nebo nosičích (papír, elektronické médium nebo lidská mysl). Vyjádření těchto faktů je vhodné pro další zpracování (1).

Informace

Informace vznikají poté, co data dostanou nějakou souvislost. Mají tedy základ v samotných datech. Informace jsou na rozdíl od dat výsledkem určitého procesu jejich zpracování. To znamená, že informace může být brána jako data, ale data se bez přidané hodnoty informací nestanou (1).

Informační management

Je soubor činností, které vedou ke splnění cílů zpracováním a vytvářením dat v organizaci. Obsahuje všechny úlohy managementu (kontrolu, vedení, plánování), které se zabývají zpracováním, získáváním, přenosem a uložením informací. Informační management lze charakterizovat jako vědomý proces, při němž jsou shromažďována data, která jsou využívána pro podporu řídících a rozhodovacích procesů na všech úrovních řízení organizace (1).

Informační systém

Pro informační systém existuje mnoho definic. Obecně lze říci, že informační systém představuje systém vzájemně propojených procesů a informací, které s těmito informacemi pracují (2).

Informační technologie

Jedná se o hardwarovou a softwarovou část, která umožňuje získávat, uchovávat a zpracovávat data za účelem distribuce informací pro potřeby uživatelů (3).

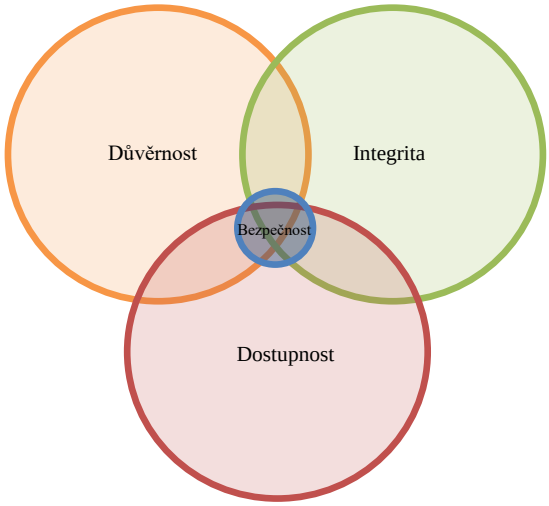
Bezpečnost IS/ICT

Jedná se o ochranu aktiv, která jsou součástí informačního systému organizace podporovaného informačními a komunikačními technologiemi (4).

Bezpečnost informací

Principem bezpečnosti informací je stanovení zásady nakládání s informacemi a způsob jejich ochrany. Nezabývá se pouze bezpečností informačních systémů a informačních komunikačních technologií, ale například i správou nedigitálních dat, způsobem zpracování dat nebo zásadami pro bezpečnou destrukci materiálů (4). Zkráceně lze říci, že se jedná o zachování důvěrnosti, dostupnosti a integrity informací (2). Na Obrázku **1** je vidět princip bezpečnosti informací.

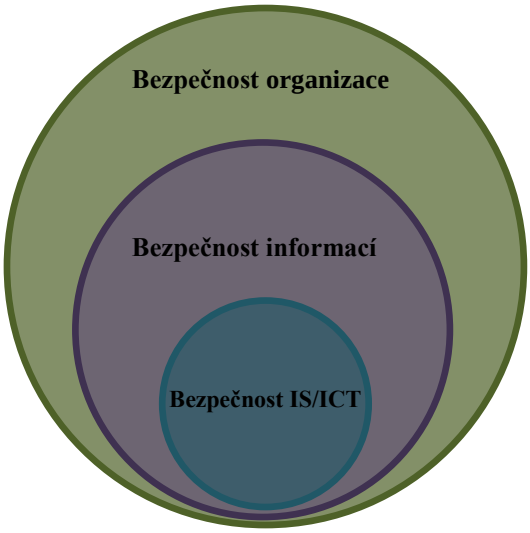
- Důvěrnost – jedná se o prevenci neoprávněnému užití informace (zajištění přístupnosti k informaci pouze oprávněnému uživateli).
- Dostupnost – oprávněný uživatel má možnost přístupu k informaci v požadovaném okamžiku.
- Integrita – zajištění správnosti, úplnosti a přesnosti informace a provedení opatření proti jejich neautorizované změně (2).



Obrázek 1: Bezpečnost informací. Zdroj: (2)

Bezpečnost organizace

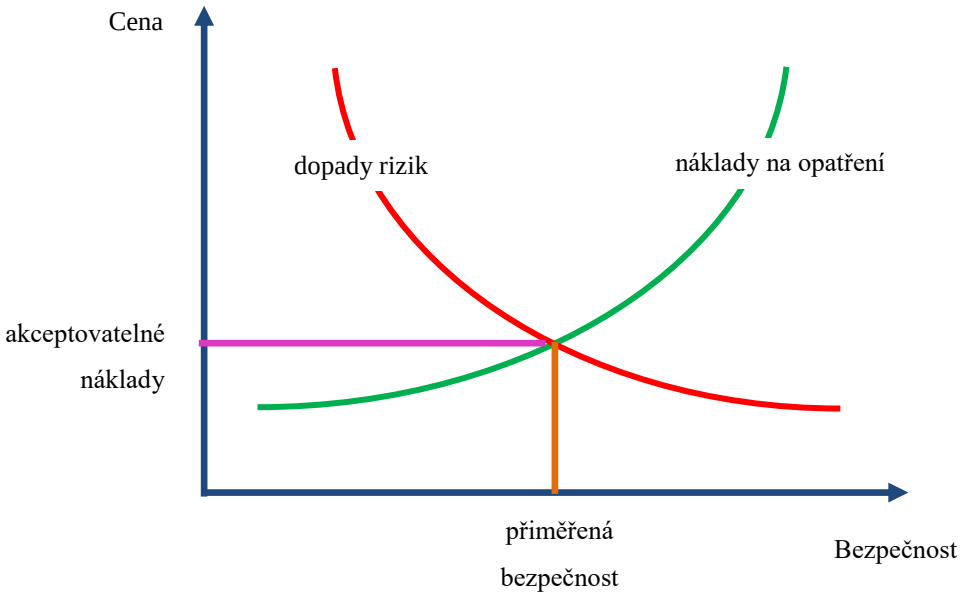
Bezpečnost organizace je nejvyšší úrovní bezpečnosti. Jejím cílem je zajištění bezpečnosti majetku a objektů organizace (například řízení fyzického přístupu), díky čemuž může pomáhat ostatním úrovním (2). Vzájemné vztahy nadřízenosti a podřízenosti lze vidět na Obrázku **2**.



Obrázek 2: Vzájemné vztahy bezpečností organizace. Zdroj: (2)

Přiměřená bezpečnost

Je stav bezpečnosti, kdy investice a úsilí vynaložené na bezpečnost musí odpovídat hodnotě aktiv a míře rizik, které mohou vzniknout. Přiměřená bezpečnost se ve většině případů stanovuje v bezpečnostní politice organizace (2). Graf přiměřené bezpečnosti za akceptovatelné náklady je vyobrazen na Obrázku **3**.



Obrázek 3: Graf přiměřené bezpečnosti za akceptovatelné náklady. Zdroj: (2)

Aktivum

Představuje hmotný a nehmotný majetek, který má pro organizaci nějakou hodnotu.

- Hmotná aktiva – jsou především technické prostředky výpočetní techniky (pracovní stanice, pasivní a aktivní prvky počítačové sítě, faxy, tiskárny, servery, záložní disky atd.).
- Nehmotná aktiva – mají spíše formu důležitých dat, programového vybavení organizace, pracovních postupů v oblasti IS/ICT nebo jiných služeb (4).

Hrozba

Hrozbu v oboru bezpečnosti informací lze chápat jako potencionální příčinu nežádoucí události, která může způsobit poškození systému a jeho aktiv (například zničení, nežádoucí zpřístupnění, modifikaci dat nebo nedostupnost služeb (5).

Potencionální schopností hrozby je způsobení nežádoucího incidentu, kvůli kterému může dojít k poškození systému nebo organizace a jejich aktiv. Hrozby můžeme rozdělit do několika základních skupin (2).

Hrozby podle zdroje:

- vnější – hacker, cracker,
- vnitřní – pomstychtivý zaměstnanec, selhání zaměstnance.

Hrozby podle úmyslu:

- úmyslné – krádež, zcizení,
- náhodné – selhání hardwaru, vymazání dat.

Hrozby podle jejich původu:

- lidský faktor – chyba uživatele, odposlech, kybernetický útok,
- přírodní – zemětřesení, povodně, blesk, požár, tornádo.

Hrozby podle dopadu na systém:

- aktivní – přesměrování komunikace,
- pasivní – odposlech.

Zranitelnost

Představuje slabé místo aktiva nebo opatření, které může být využito hrozbou, čímž se hodnota aktiva může zničit nebo snížit (4).

Riziko

Je kombinace pravděpodobnosti vzniku událostí a jejího následku. Výsledná hodnota se snižuje zavedením opatření pro dané zranitelnosti a hrozby (4).

Dopad

Dopad je vznik jakékoliv škody na aktivu působením hrozby (2).

Opatření

Aktiva, která umožňují snížit hodnotu hrozby nebo jí úplně eliminovat (1).

Bezpečnostní událost

Zjištěný výskyt stavu systému, sítě nebo služby označující možné narušení politiky bezpečnosti informací nebo selhání opatření nebo předem neznámá situace, která může být pro bezpečnost závažná (6). Zjednodušeně lze říci, že je událost příčina incidentu.

Bezpečnostní incident

Jedná se o jednotlivou nežádoucí nebo neočekávanou událost bezpečnosti informací, která může s významnou pravděpodobností vyvolat kompromitování operací souvisejících s činností organizace a ohrožení bezpečnosti informací (6).

Standard

Úmluva obsahující technické specifikace nebo jiná stanovená kritéria používaná jako pravidla nebo směrnice. Bývají nástrojem dynamického prosazování politiky technického směru a následného pokroku (3).

Norma

Jedná se o doporučení použitelných standardů k realizaci požadovaného kompatibilního řešení. V oblasti ICT se jedná o směrnice nebo předpisy vydávané různými konsorcii uživatelů a výrobců, které jsou většinou výsledkem náročně dosaženého kompromisu (3).

2.2 Normalizační instituce

ISO - International Organization for Standardization

ISO je nezávislá, nevládní a mezinárodní organizace se členstvím ve 161 národních normalizačních orgánech. Prostřednictvím svých členů ISO sdružuje odborníky, kteří sdílejí své znalosti a rozvíjejí dobrovolné, koncesně založené a tržně relevantní Mezinárodní standarty, které podporují inovace a poskytují řešení globálních výzev (7).

IEC - International Electrotechnical Commision

Společnost IEC (Mezinárodní elektrotechnická komise), která byla založena v roce 1906, je přední světovou organizací pro přípravu a zveřejňování mezinárodních norem pro všechny elektrické, elektronické a související technologie. Známé jako "elektrotechnologie" (8).

ITU - International Telecommunications Union

Je to mezinárodní organizace spadající do hierarchie OSN. Mezi hlavní úkoly Unie patří udržovat a prohlubovat mezinárodní spolupráci ve všech oblastech telekomunikačního sektoru za účelem zlepšení a racionalizace využití všech druhů telekomunikačních služeb, podporovat rozvoj odpovídajících technických prostředků, dbát o účelné rozdělování kmitočtového spektra a koordinaci jeho využívání, zajišťovat technickou pomoc v oblasti telekomunikací rozvojovým zemím. Činnost ITU je rozdělena podle odbornosti

do tří sektorů: radiokomunikace, standardizace telekomunikací a rozvoj telekomunikací (9).

UNMZ - Úřad pro technickou normalizaci, metrologii a státní zkušebnictví

Je správní úřad České republiky, který je podřízen Ministerstvu průmyslu a obchodu České republiky. Úřad byl zřízen zákonem č. 20/1993 Sb., o zabezpečení výkonu státní správy v oblasti technické normalizace, metrologie a státního zkušebnictví. Zabezpečuje úkoly vyplývající z usnesení vlády č. 631 ze dne 9. listopadu 1994, o zajištění procesu integrace ČR do EU včetně harmonizace právního řádu s EU a sbližování technických předpisů a norem z EU (10).

ČSN (česká technická norma) vzniká dvěma způsoby (2):

- tvorbou původních ČSN vyplývajících z národních potřeb a z hledisek zachování funkčního fondu ČSN,
- přejímáním evropských a mezinárodních norem do soustavy českých technických norem formou ČSN EN (ČSN ISO, ČSN IEC, atd.).

2.3 Normy v oblasti informační bezpečnosti

Pro budování bezpečnosti informací je vytvořena řada norem ISO/IEC 27000, která vychází z konceptu PDCA (blíže popsán v Kapitole **2.4.2**).

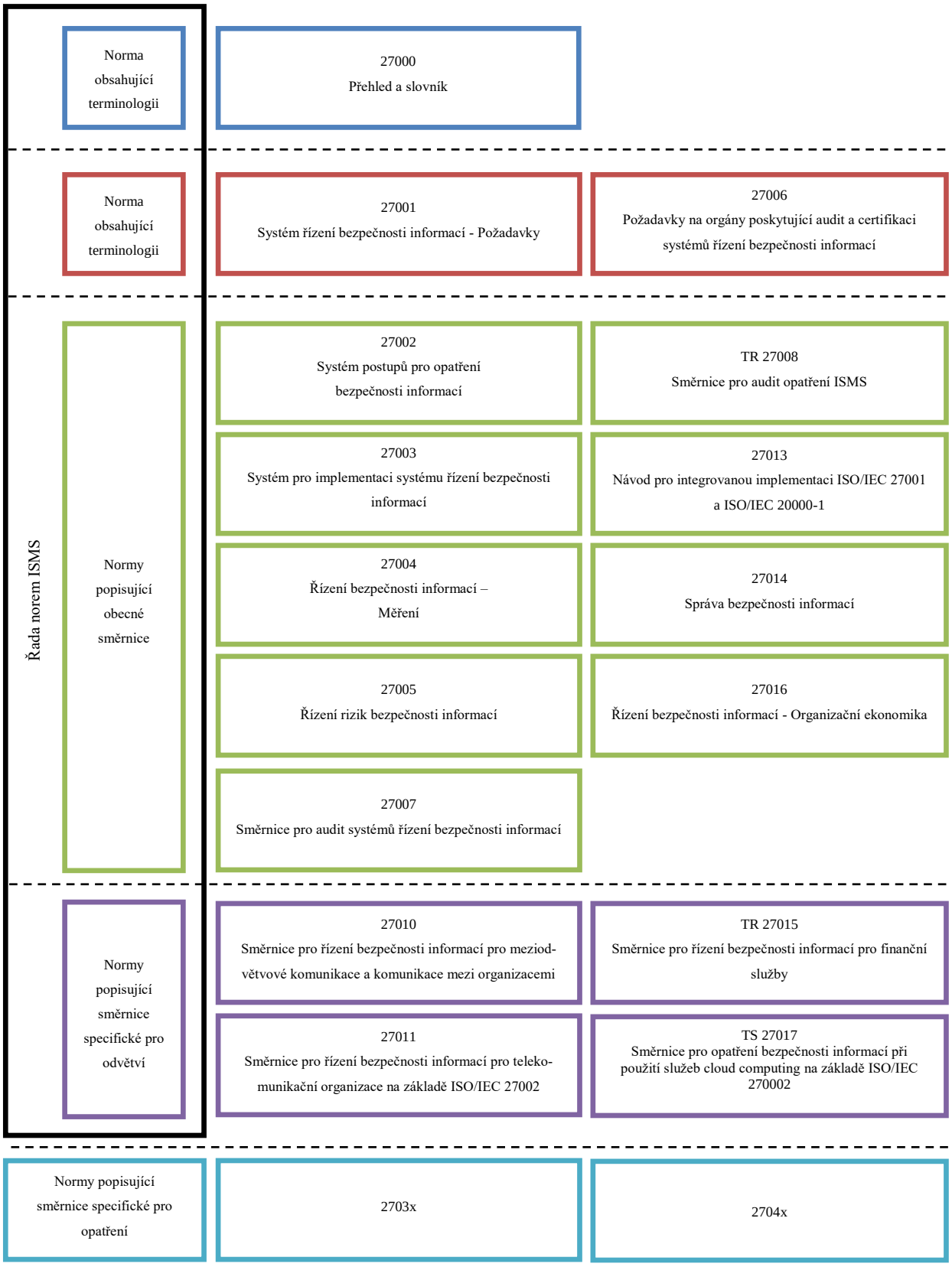
Řada norem ISMS zahrnuje normy, které (6):

- stanovují požadavky na ISMS a na pracovníky, kteří takové systémy certifikují,
- poskytují přímou podporu, podrobný návod nebo interpretaci pro celkový proces ustanovení, implementování, udržování a zlepšení ISMS,
- se zabývají směrnicemi pro ISMS specifickými pro jednotlivá odvětví,
- se zabývají posuzováním shody ve vztahu k ISMS.

2.3.1 Normy řady ISO/IEC 27000

- ISO/IEC 27000 – přehled a slovník,
- ISO/IEC 27001 – požadavky,
- ISO/IEC 27002 – soubor postupů pro opatření bezpečnosti informací,
- ISO/IEC 27003 – směrnice pro implementaci systému řízení bezpečnosti informací,
- ISO/IEC 27004 – řízení bezpečnosti informací (měření),
- ISO/IEC 27005 – řízení rizik bezpečnosti informací,
- ISO/IEC 27006 – požadavky na orgány poskytující audit a certifikaci systémů řízení bezpečnosti informací,
- ISO/IEC 27007 – směrnice pro audit systémů řízení bezpečnosti informací,
- ISO/IEC 27008 – směrnice pro audit opatření ISMS,
- ISO/IEC 27009 – definuje požadavky používání ISO/IEC 27001 ve specifických odvětvích,
- ISO/IEC 27010 – směrnice pro řízení bezpečnosti informací pro meziodvětvové komunikace a komunikace mezi organizacemi,
- ISO/IEC 27011 – směrnice pro řízení bezpečnosti informací pro telekomunikační organizace na základě ISO/IEC 27002,
- ISO/IEC 27013 – návod pro integrovanou implementaci ISO/IEC 27001,
- 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 (6)).

Na Obrázku **4** lze vidět vzájemné vztahy mezi normami řady ISMS a dále jsou podrobněji popsány normy, které byly v práci využity.



Obrázek 4: Vztahy mezi normami řady ISMS. Zdroj: (6)

ISO/IEC 27000

Norma poskytující přehled systémů řízení bezpečnosti informací a s tím souvisejících termínů, pojmů a definic. Jsou v ní uvedeny obecné termíny a definice související s ISMS. Lze ji uplatnit v jakýchkoli typech a velikostech organizací (6).

ISO/IEC 27001

Tato norma poskytuje podporu při ustanovení, implementaci, udržování a neustálé zlepšování systému řízení bezpečnosti informací. Z toho důvodu patří do strategických plánů a rozhodnutí organizací, které se chystají zavést systém řízení bezpečnosti informací. Ustanovení systému řízení bezpečnosti informací ovlivňuje několik faktorů, u kterých je možné, že se budou časem měnit. Do těchto faktorů lze například řadit: požadavky na bezpečnost, potřeby a cíle organizace atd. Norma klade důraz na zavedení procesního přístupu k řešení ISMS a zavádí model PDCA, který může být aplikován na všechny procesy, které jsou v normě obsaženy (11).

ISO/IEC 27002

Tato norma je určena pro organizace k použití jako doporučení pro výběr opatření v rámci procesu zavádění systému řízení bezpečnosti informací, založeného na normě ISO/IEC 27001, nebo jako pokyny pro organizace implementující obecně přijatá opatření bezpečnosti informací. Tato norma je také určena pro použití při vyvíjení směrnic pro řízení bezpečnosti informací specifických pro průmysl a organizace, s přihlédnutím k jejich konkrétnímu prostředí rizik pro bezpečnost informací. Vhodnost aplikace jednotlivých opatření je stanovena na základě analýzy rizik a jejich implementace je závislá na konkrétní situaci v organizaci. Cílem není implementovat všechna opatření, která norma obsahuje a popisuje, ale dojít k aplikovatelným cílům jednotlivých opatření. Obsahuje 114 bezpečnostních opatření rozdělených do těchto 14 oblastí (12):

- A.5 - Politiky bezpečnosti informací
- A.6 - Organizace bezpečnosti informací
- A.7 - Bezpečnost lidských zdrojů
- A.8 - Řízení aktiv
- A.9 - Řízení přístupu
- A.10 - Kryptografie

- A.11 - Fyzická bezpečnost a bezpečnost prostředí
- A.12 - Bezpečnost provozu
- A.13 - Bezpečnost komunikací
- A.14 - Akvizice, vývoj a údržba systémů
- A.15 - Dodavatelské vztahy
- A.16 - Řízení incidentů bezpečnosti informací
- A.17 - Aspekty řízení kontinuity činnosti organizace z hlediska bezpečnosti informací
- A.18 - Soulad s požadavky

ISO/IEC 27003

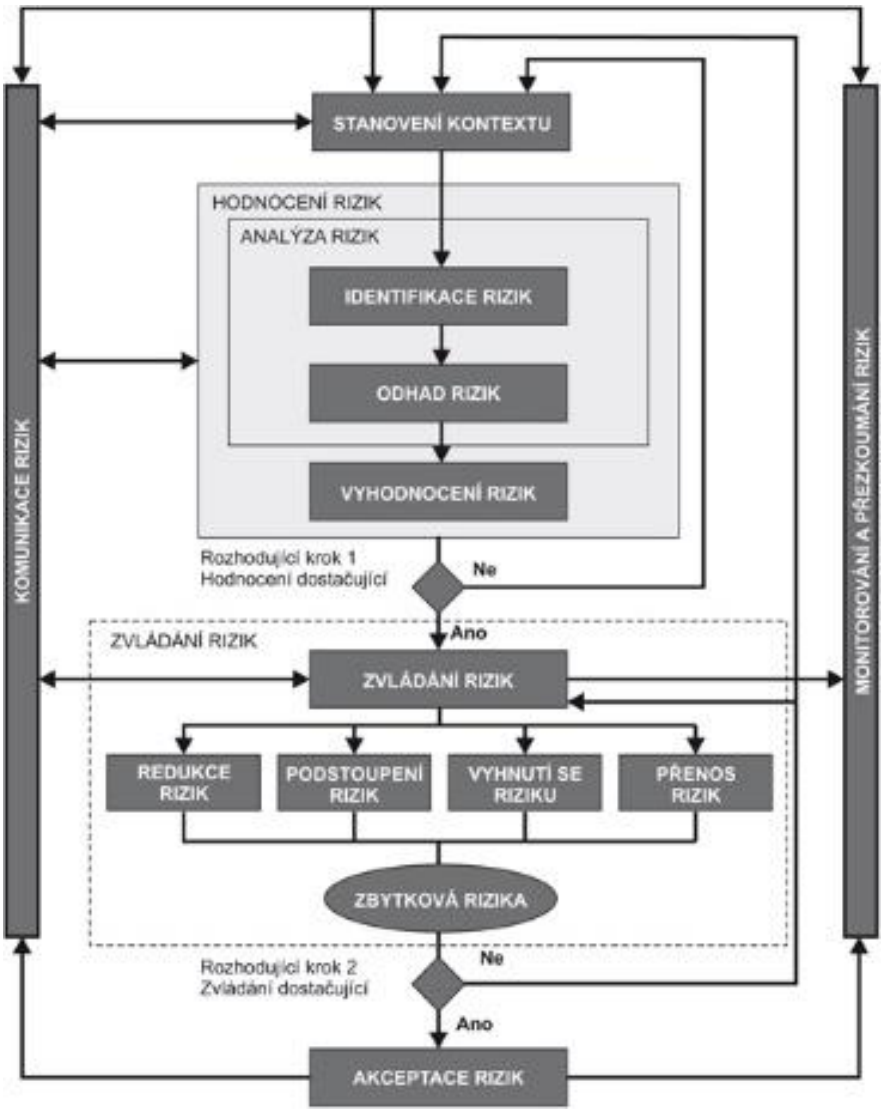
Zaměřuje se na kritické aspekty nutné pro úspěšný návrh a implementaci systému řízení bezpečnosti v souladu s ISO/IEC 27001. Popisuje proces návrhu ISMS od začátku až po vytvoření implementačního plánu. Obsahuje proces získání souhlasu vedení organizace k zavedení ISMS, definuje projekt jak implementovat ISMS a poskytuje doporučení, jak plánovat projekt ISMS, aby výsledkem byl finální plán implementace ISMS. Dále také obsahuje provedení analýzy požadavků bezpečnosti informací, hodnocení rizik, plánování zvládání rizik a také návrh ISMS. Tuto normu lze aplikovat na různorodé organizace, které mohou danou normu doplnit o své potřeby nebo ji naopak zjednodušit (13).

ISO/IEC 27004

Tato norma poskytuje doporučení pro vývoj a použití metrik za účelem hodnocení účinnosti zavedeného systému řízení bezpečnosti informací a opatření nebo skupiny opatření, jak je uvedeno v ISO/IEC 27001. Aplikace těchto doporučení je prováděna v programu měření bezpečnosti informací a zahrnuje tyto procesy: rozvoj metrik, měření, analýzu výsledků předešlých měření, vyhodnocení měření a následné zlepšování (14).

ISO/IEC 27005

Norma poskytující doporučení pro řízení rizik bezpečnosti informací v rámci organizace. Podporuje obecný koncept specifikovaný v normě ISO/IEC 27001 a je strukturována, aby dostatečně podporovala implementaci informační bezpečnosti založené na přístupu řízení rizik. Je aplikovatelná na všechny typy organizací, které chtějí řídit rizika bezpečnosti informací (15). Souhrnný pohled na proces řízení rizik je uveden na Obrázku 5.



Obrázek 5: Proces řízení rizik. Zdroj: (16)

2.4 Systém řízení bezpečnosti informací

Systém řízení bezpečnosti je součástí systému řízení celé organizace, který se zaměřuje na ustanovení, zavádění, provoz, monitorování, přezkoumání, údržbu a zlepšování bezpečnosti informací. Tento systém bezpečnosti v sobě obsahuje politiky, organizační strukturu, plánování, odpovědnosti uživatelů, mechanismy, postupy procesy a zdroje (4). Pro svoje činnosti využívá model PDCA (blíže popsán v Kapitole **2.4.2**). Díky úspěšnému zavedení ISMS může organizace získat (6):

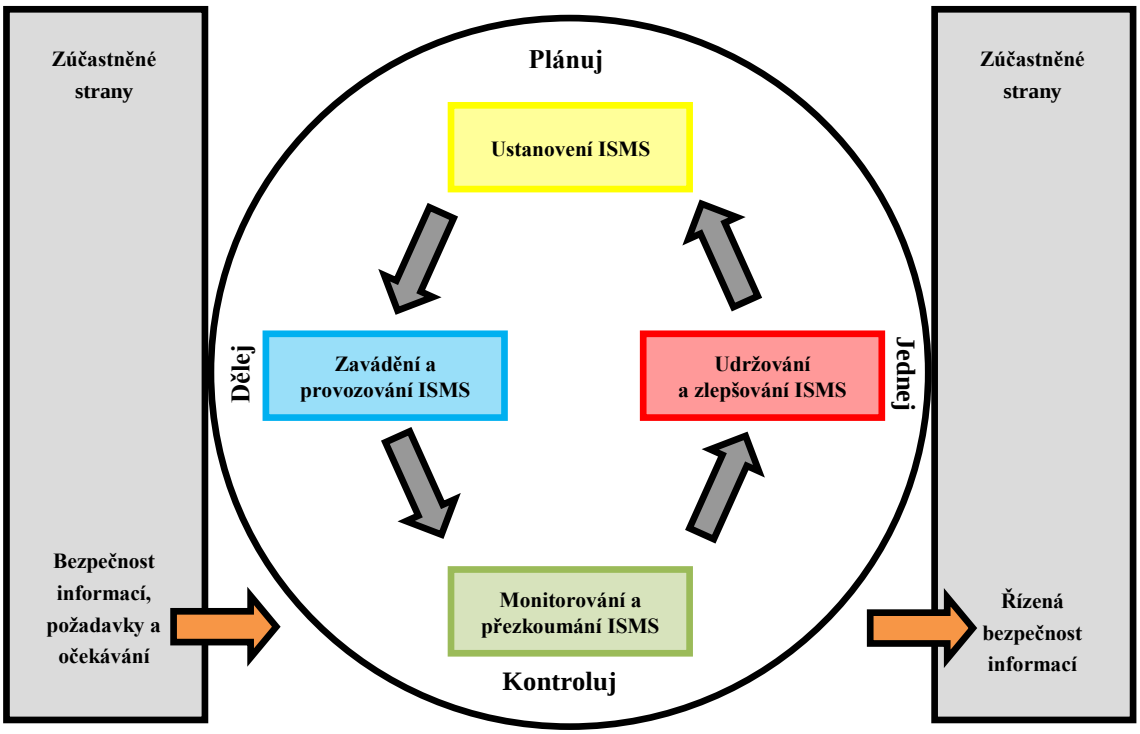
- větší záruku, že její informační aktiva budou neustále adekvátně chráněna před hrozbami,
- zvýšení povědomí zaměstnanců organizace o důležitosti odpovědného chování při nakládání s citlivými údaji,
- neustále zlepšované prostředí, ve kterém se řízení bezpečnosti informací provádí,
- lepší udržování strukturovaného a komplexního rámce pro identifikování a posuzování rizik bezpečnosti informací, výběr a následnou implementaci vybraných opatření, monitorování a zvyšování efektivnosti aplikovaných opatření,
- splnění zákonného požadavku na systémové zajištění bezpečnosti práce při používání citlivých údajů.

2.4.1 Etapy zavádění ISMS

Na implementaci ISMS v organizaci existují následující kroky: ustanovení, zavádění, provoz, monitorování, přezkoumávání, udržování a zlepšování. Ke všem krokům musí existovat důkladná dokumentace. Při procesu zavádění ISMS v organizaci (popsán v ISO/IEC 27001) se vychází z modelu PDCA (6).

2.4.2 Demingův cyklus - PDCA

Demingův cyklus PDCA (Plan-Do-Check-Act) je iterativní metoda, která je používaná při zavádění a postupném zlepšování kvality služeb, procesů a výrobků. Jedná se o model cyklu, který opakuje čtyři základní činnosti (plánuj, dělej, kontroluj a jednej). Tento koncept zformuloval a použil americký statistik William Edwards Demin. V současné době je tento model používán jako základní kámen mezinárodních standardů (4). ISMS využívá PDCA modelu, který se skládá z čtyř částí. Tyto části jsou popsány dále a lze je vidět na Obrázku **6**.



Obrázek 6: Model PDCA cyklu v ISMS. Zdroj: (17)

Plánuj – Ustanovení ISMS

V této první fázi dochází ke stanovení požadavků na rozsah aplikace ISMS podle činností, které organizace provádí, zpracovává se bezpečnostní politika a bezpečnostní dokumentace, nastavuje se strategie ISMS, vnitřní směrnice a časový harmonogram projektu pro zajištění návaznosti činností a jednotlivých etap. Důležitou částí této fáze je i odsouhlasení všech dokumentů, plánů a postupů vedením organizace (4).

Dělej – Zavádění ISMS

Tato fáze se soustředí na prosazování bezpečnostních opatření tak, jak byla navržena v první fázi. Je důležité, aby všechna bezpečnostní opatření byla uvedena v příručce bezpečnosti informací. Dále se vytváří plán zvládání rizik, definuje se plán pro budování bezpečnostního povědomí, zavádí se bezpečnostní opatření, upřesňují se způsoby měření a sledování účinnosti bezpečnostních opatření a vytváří se postupy pro zvládání bezpečnostních incidentů (4).

Kontroluj – Monitorování a přezkoumávání ISMS

V této fázi dochází ke zpracování metodiky kontroly účinnosti ISMS formou interních auditů. Data z předchozí fáze jsou analyzována a dále zkoumána. Musí být prováděny testy techniky, kontrola zaměstnanců, penetrační testy, revize smluv o poskytování služeb s třetími stranami atd. Výsledky jednotlivých testů jsou porovnávány s očekávanými výsledky (4).

Jednej – Udržování a zlepšování ISMS

Na základě výsledků předchozí fáze dochází ke zlepšení ISMS a k nápravě neshod, které vyplývají z přezkoumání systému řízení ze strany vedení organizace v předchozí etapě. Jsou tedy zaváděna preventivní a nápravná opatření pro odstranění nedostatků. Touto etapou dochází k procesu tzv. neustálého zlepšování ISMS (4).

2.4.3 Ustanovení ISMS

V této etapě se definují základy celého ISMS. V rámci ustanovení ISMS by se měly splnit tyto požadavky (6):

- Analýza organizace, která obsahuje určení činností organizace, její umístění používané technologie, aktiva a vnitřní uspořádání. Na základě provedené analýzy se stanoví hranice a rozsah zaváděného ISMS. Jestliže jsou nějaké části organizace vyjmuty z procesu ISMS musí se zaznamenat důvody tohoto počínání.
- Ze stanoveného rozsahu zaváděného ISMS je následně nutné stanovit politiku ISMS. Politika musí obsahovat požadavky plynoucí z činností organizace a ze zákonů dané země, dále směr a cíle činností v okruhu bezpečnosti informací.

- Dále je nutné stanovit, jak bude probíhat hodnocení rizik a podle jakých měřítek budou určena rizika pro akceptaci. Postup vybraný pro hodnocení rizik musí zajišťovat možnost porovnání a opakování zjištěných výsledků.
- Dalším krokem je identifikování všech aktiv, určení vlastníků aktiv, nalezení hrozeb působící na aktiva a nalezení zranitelných míst. Musí se stanovit, jaký vliv bude mít na aktiva ztráta důvěrnosti, integrity a dostupnosti.
- Následně je provedena analýza a vyhodnocení rizik. Určuje se, jak bude zacházeno s identifikovanými riziky (opatření nebo akceptace). Dále se aplikují opatření na vybraná rizika, která nemohou být akceptovaná a bez jakéhokoli zásahu.
- Dále jsou určeny cíle jednotlivých opatření, kde se musí zdůvodnit stanovená opatření podle hodnocení a zvládání rizik.
- Ostatní rizika jsou akceptována a vše musí být odsouhlaseno vedením organizace.
- Vedení musí poté dát povolení k zavedení a provozu ISMS.
- V posledním kroku je sepsáno tzv. „Prohlášení o aplikovatelnosti“. To shrnuje předchozí kroky a jsou zde zapsány cíle, vybraná opatření společně se stanovenými důvody, aplikovaná opatření použité v organizaci a vyloučená rizika s odůvodněním.

2.4.4 Zavádění a provoz ISMS

V této etapě dochází k prosazování všech bezpečnostních opatření tak, jak byla analyzována a navržena v etapě předchozí. Během této etapy je nutné provést dále popsané činnosti.

Plán zvládání rizik

Dokument, který popisuje všechny činnosti ISMS, které jsou potřebné pro řízení bezpečnostních rizik, stanovené priority a cíle těchto činností, omezující faktory a potřebné zdroje. Dále musí být definovány odpovědnosti za provádění jednotlivých činností, které jsou naplánované. Při tvorbě plánu je vycházeno z výsledků řízení rizik, které jsou sepsány v dokumentu o hodnocení rizik a v prohlášení o aplikovatelnosti a dále také z pravidelného přezkoumávání ISMS organizace (4).

Příručka bezpečnosti informací

Tato příručka představuje souhrn dokumentů, které obsahují stanovení bezpečnostních pravidel, zásad, principů a odpovědnosti. Při sestavování tohoto dokumentu je nutné vytvořit provedení pro každou cílovou skupinu tak, aby každá skupiny měla dokument s odpovídajícím zaměřením a podrobností. Dokument musí být pro dané cílové skupiny lehce srozumitelný a pochopitelný (4).

Bezpečnostní povědomí a jeho prohlubování

V rámci rozvoje ISMS se jedná o velice důležitou činnost a mělo by být prioritou. Dle zkušeností z praxe je nejslabším článkem v oblasti bezpečnosti lidský faktor. Z toho důvodu je důležité neustále budovat a prohlubovat bezpečnostní povědomí u zaměstnanců a dalších zainteresovaných stran. Z důvodu rozvoje ISMS a obměnou pracovníků je budování bezpečnostního povědomí trvalý a nikdy nekončící proces a v mnoha případech může rozhodovat o skutečné efektivitě zavedeného ISMS. Součástí školení by například mělo být: názvosloví (aktivum, informační bezpečnost, analýza rizik, hrozba, dopad, atd.), co je to ISMS (vysvětlení a jeho přínosy), bezpečnostní politika, dokument pravidel (bezpečnostní pravidla pro uživatele), novinky a změny oproti předchozímu školení, testování znalostí jednotlivých uživatelů (test, ústní pohovory). Zaměstnanci musí být proškolování při vzniku pracovního poměru a dále v jeho průběhu. Školení musí být realizováno s ohledem na zaměření činností jednotlivých zaměstnanců (4).

Měření provozu ISMS

Pro zjišťování efektivnosti ISMS je nutné měřit nějakým způsobem účinnosti zavedených bezpečnostních opatření. Je potřeba pravidelně sledovat stanovené ukazatele, které nám poskytují informace o skutečném fungování systému řízení bezpečnosti. Na základě získaných informací pak lze zjišťovat efektivnost a následně provádět důležitá rozhodnutí nebo opatření. Při měření se opět používá PDCA modelu, kdy se jeho proces neustále zlepšuje a zpřesňuje (4).

Řízení dokumentace ISMS

Posledním krokem zavádění ISMS je řízení dokumentace. Je nutné, aby o každém kroku byly shromažďovány podklady pro další fázi monitorování. Pro realizaci kontroly fungování a účinnosti ISMS je důležité vytvořit pravidla pro tvorbu, distribuci, schvalování a aktualizaci dokumentace řízení bezpečnosti. Současně se v této dokumentaci provádí záznam informací o provedené činnosti. V těchto informacích o provedení činnosti jsou zaznamenávány osoby, které dané činnosti prováděly, datum, čas, místo a výsledky činnosti, která byla provedena (4).

2.4.5 Monitorování a přezkoumání ISMS

Ve třetí etapě se zajišťuje zpětná vazba při zavedení ISMS, ve které se ověřují všechny aplikované bezpečnostní opatření a jejich důsledky na ISMS. Opět má monitorování a přezkoumání několik kroků (4):

- Probíhá zde monitorování, kontrolování a v případě potřeby se zavádí nová opatření pro detekci chyb při zpracování a pro identifikaci pokusu o narušení. Díky monitorování může vedení organizace posuzovat, jestli pověřené osoby a použité technologie správně plní svoji roli. Dále se zjišťuje, jestli jsou zavedená opatření dostatečně spolehlivá proti narušení.
- Dále se provádí pravidelné přezkoumávání účinnosti ISMS, které jsou zaměřena na splnění politiky, opatření a cílů. Zahrnují se do nich i výsledky incidentů, auditů a měření účinnosti opatření.
- V dalším kroku se z měření implementovaných opatření zjišťuje, jestli jsou splněny požadavky bezpečnosti..
- Nutné je, aby se v pravidelných intervalech přezkoumávala rizika. Zjišťuje se, jestli nevznikají nová rizika nebo se nezměnila váha dříve zjištěných rizik, vzhledem ke změně v organizaci, nebo nově vzniklé hrozbě.
- Provádí se audity v pravidelných intervalech, jejichž náplň pokryje celý rozsah ISMS.
- Vedení organizace provádí přezkoumávání ISMS, aby se dodržel ideální rozsah opatření a ISMS se mohlo případně aktualizovat a tím zlepšovat. Interval přezkoumávání by neměl přesahovat více jak jeden rok.

2.4.6 Udržování a zlepšování ISMS

V této poslední fázi dochází ke sběru podnětů ke zlepšování a k nápravě všech nedostatků, které se v ISMS vyskytují. Tímto dochází k neustálému vývoji a zlepšování ISMS. Během této fáze by se měly provést následující činnosti (4):

- zavádět identifikované možnosti zlepšení ISMS,
- implementovat odpovídající opatření k nápravě nedostatků (je nutné vzít v potaz všechny souvislosti a opatření realizovat tak, aby se omezily možnosti jejich opakování),
- implementovat preventivní opatření pro odstranění budoucích nedostatků (toto spočívá v proaktivní formě řešení, kdy se zavádí opatření na nedostatky, které ještě nenastaly). Při odstraňování nedostatků je potřeba vzít v úvahu všechny souvislosti a opatření realizovat tak, aby se redukovaly možnosti jejich opakování,
- zdokumentování a přezkoumání, zda jsou zavedené postupy účinné.

2.5 Metodiky

2.5.1 ITIL - Information Technology Infrastructure Library

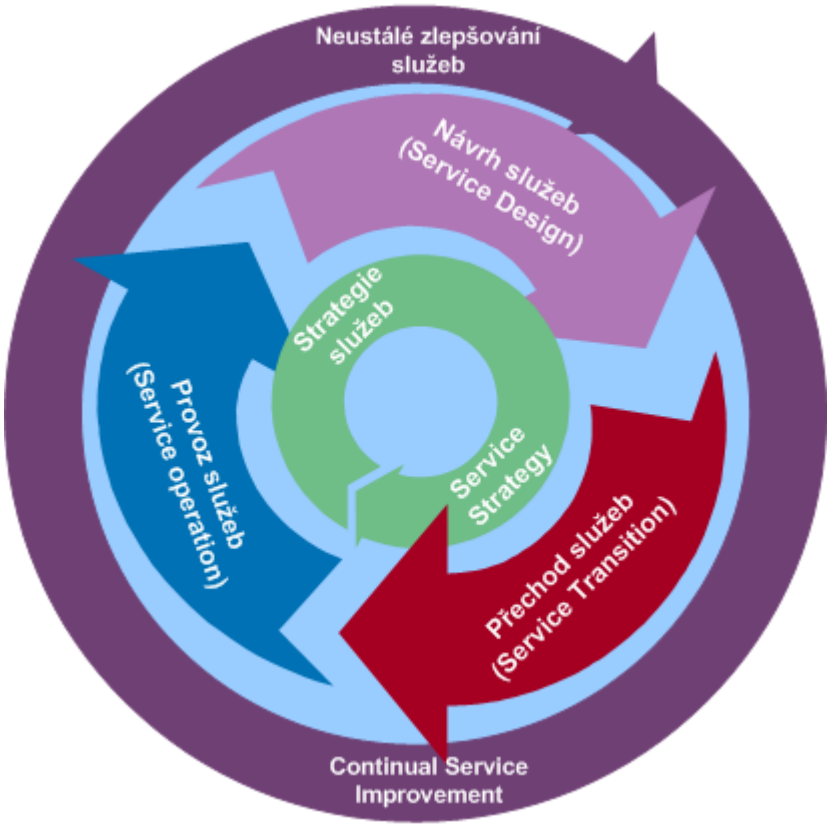
Je knihovna přístupů pro oblast řízení IT služeb a souvisejících procesů sloužící k zajištění dodávky kvalitních IT služeb za přiměřené náklady (Obrázek 7). Obsahuje doporučení a osvědčené postupy vycházející z nejlepších praktických zkušeností mnoha společností a soustřeďuje se na plánování, modifikaci, vytváření, správu, dodávku, analýzu a použití služeb IT. ITIL spravuje Office of Government Commerce. Knihovna ITIL se dnes považuje za mezinárodní standard pro oblast řízení IT služeb (2). V novodobé formě má ITIL označení V3 a je rozdělena na několik částí (knih) zaměřených na specifickou oblast řízení IT služeb (5 knih popisující 26 procesů (18)):

- Strategie služeb (Service Strategy) – kniha se zabývá problematikou IT Governance a je určena pro osoby na pozici ředitele IT. Popisuje 3 základní procesy: správu financí (financial management), správa portfolia služeb (service portfolio management) a správa požadavků (demand management).
- Návrh služeb (Service Design) – tato kniha se zaměřuje na návrh služeb, které uspokojí současné i budoucí požadavky businessu. Skládá se z těchto částí:

    - Správa katalogu služeb (Service Catalogue Management)
    - Správa úrovně služeb (Service Level Managemen)
    - Správa kapacit (Capacity Managemen)
    - Správa dostupnosti (Availability Management)
    - Správa kontinuity služeb IT (IT Service Continuity Management)
    - Správa bezpečnosti informací (Information Security Management)
    - Správa dodavatelů (Supplier Management)
- Implementace služeb (Service Transition) – tato publikace řeší problematiku dodávky služby požadované businessem až do produkčního prostředí. Jsou v ní popsány následující procesy:
    - Správa změn (Change Management)
    - Správa aktiv a konfigurace (Service Asset and Configuration Management)
    - Správa znalostí (Knowledge Management)
    - Plánování a podpora přechodu (Transition Planning and Support)
    - Správa release a nasazení (Release and Deployment Management)
    - Ověření a testování služby (Service Validation and Testing)
    - Vyhodnocení (Evaluation)
- Provoz služeb (Service Operation) – zabývá se problematikou dodávky služeb v požadované kvalitě. Píše se o těchto procesech:
    - Správa událostí (Event Management)
    - Správa incidentů (Incident Management)
    - Správa problémů (Problem Management)
    - Správa přístupů (Access Management)
    - Provádění požadavků (Request Fullfilment)
    - Správa provozu IT (IT Operation Management)
    - Správa aplikací (Application Management)
    - Technická správa (Technical Management)
- Průběžné zlepšování služeb (Continual Service Improvement) – zaměřuje se na:
    - Měření služeb (Service Measuremen)
    - Vykazování služeb (Service Reporting)

Hlavní přínosy procesního řízení dle ITIL (19):

- zvýšená spokojenost uživatelů a zákazníků se službami IT,
- zlepšená dostupnost služeb,
- finanční úspory plynoucí ze snížení opakovaných prací, ztraceného času, zlepšené správy a využití zdrojů,
- zkrácení času pro uvedení nových produktů a služeb na trh,
- zlepšení podkladů pro rozhodování a optimalizace rizik.

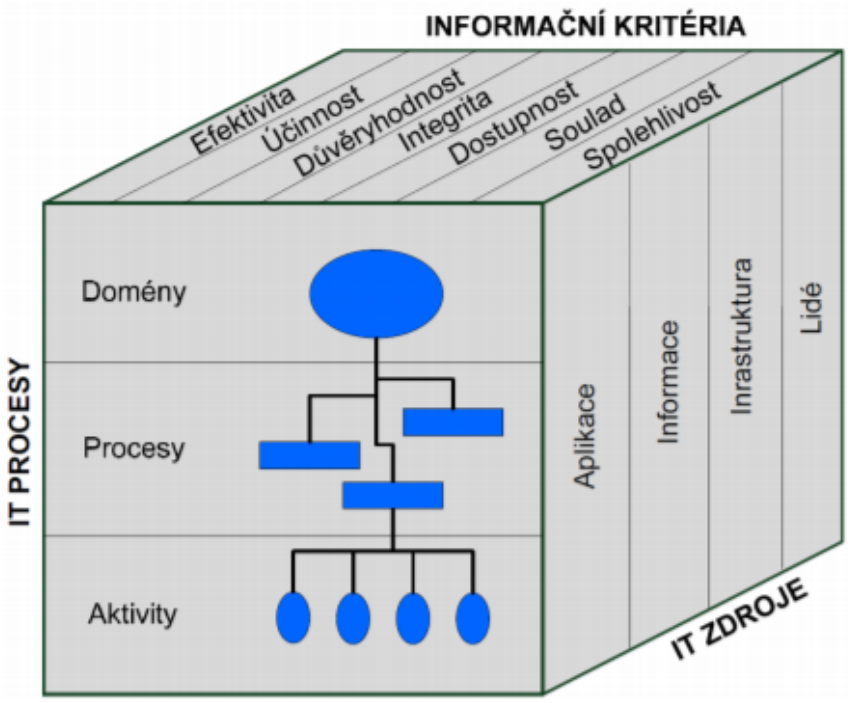


Obrázek 7: Procesní řízení IT. Zdroj: (19)

2.5.2 COBIT

COBIT (Control Objectives for Information and related Technology) je mezinárodní metodika vytvořena asociací ISACA. Tato metodika je sadou všeobecně přijímaných procesů, návodů pro hodnocení, ukazatelů a nejlepších praktických zkušeností, jejímž cílem je maximalizace užitku plynoucího z informačních technologií vlastněných organizací. Je určena spíše pro vrcholový management k posuzování fungování ICT a auditorů. Kostka COBIT (Obrázek **8**) je tvořena třemi osami, které se dělí do dalších skupin:

- IT procesy – domény, procesy, aktivity
- IT zdroje – aplikace, infrastruktura, lidé, informace
- Informační kritéria – účinnost, důvěryhodnost, integrita, efektivita, dostupnost, soulad, spolehlivost (2).



Obrázek 8: Kostka COBIT. Zdroj: (2)

Ze studií vyplývá, že metodika COBIT je komplexnější než rámec ITIL, ten však řeší některé části více detailněji. Avšak lze říci, že s vydáváním nových verzí se vzájemně sbližují (i tak si ponechávají svoje specifika vyplývající z účelu, za kterým byly navrženy). Doporučuje se kombinovat oba způsoby řízení pro splnění požadavků konkrétních prostředí (4).

2.6 Analýza rizik

V této analýze se provádí identifikace zranitelných míst v organizaci. Dále zachycuje seznam hrozeb, které na organizaci působí a stanovuje rizika příslušná každému zranitelnému místu a hrozbě. Cílem této analýzy je snížení rizik na přijatelnou úroveň, respektive akceptaci zbytkových rizik tam, kde se jejich minimalizace nevyplatí. Rizika v analýze můžeme rozlišovat na (2):

- Bezvýznamné riziko (váha 1) – není nutné zavádět opatření. Nejedná se však o riziko, které nikdy nemůže nastat, proto je nutné o riziku vědět a upozornit na něj. Riziko je možno přijmout.
- Akceptovatelné riziko (váha 2) – riziko, které je přijatelné po souhlasu vedení. Je důležité zvážit náklady na případné zlepšení nebo řešení. Pokud není možné zavést technická bezpečnostní opatření ke snížení rizika, je nutné zavést alespoň přiměřená organizační opatření (například školení). Možné riziko, zvýšit pozornost.
- Mírné riziko (váha 3) – urgentnost opatření není tak závažná, je ale nutné bezpečnostní opatření zrealizovat dle zpracovaného plánu vedení firmy. Potřeba nápravné činnosti.
- Nežádoucí riziko (váha 4) – toto riziko vyžaduje urychlené provedení odpovídajících bezpečnostních opatření, které by riziko snížily na přijatelnou úroveň. Na snížení rizika musí být přiděleny potřebné prostředky. Jedná se o vysoké riziko vyžadující bezprostřední bezpečnostní opatření.
- Nepřijatelné riziko (váha 5) - jedná se o nepřípustné, značné a kritické riziko. Hrozí permanentní možnost úrazů. Je nutné okamžitě zastavit činnosti, odstavit z provozu do doby realizace nezbytných opatření a nového vyhodnocení rizik a přijetí potřebných opatření. Činnost nemůže být zahájena a ani v ní nesmí být pokračováno, dokud riziko není sníženo. Velmi vysoké riziko, zastavení činnosti.

2.6.1 Obecný postup při provádění analýzy rizik

- Stanovení hranice revize – stanoví se, která aktiva budou do analýzy zahrnuta, abychom předešli vynakládání zdrojů na nepotřebné činnosti (2).
- Identifikace aktiv – pod zvolenou hranicí se vytvoří soupis všech identifikovaných aktiv (2).
- Ohodnocení aktiv – k předešlému seznamu aktiv je nutné přiřadit hodnoty, které zastupují význam aktiva pro činnost organizace. Není podmínkou, že je hodnota aktiva určena finančním ohodnocením, ale například z hlediska nepříznivých dopadů na činnosti organizace, plynoucí ze ztráty integrity, dostupnosti, důvěrnosti, individuální odpovědnosti, autenticity a spolehlivosti (2).
- Identifikace hrozeb – jsou vyhledávány hrozby, pro které v následujících krocích musí být zvoleno vhodné opatření. Hrozba vzniká tehdy, pokud ohrožuje alespoň jedno z aktiv, které bylo identifikované v předchozích krocích. Hrozby se identifikují mnoha způsoby (například z oborových zkušeností, z provedené analýzy nebo z literatury). Na každou organizaci působí odlišné hrozby, podle toho v jakém odvětví působí. Pro identifikaci hrozeb lze využít seznam uvedený v normě ISO/IEC 27005 v příloze C (2).
- Odhad zranitelnosti – nám odhalí slabá místa ve fyzickém prostředí, organizaci, personálu managementu, postupech, administraci softwaru, hardwaru nebo v komunikačním zařízení, která mohou být využita zdrojem hrozby a způsobit tak škodu na aktivech (2).
- Identifikace plánovaných a existujících ochranných opatření – výsledkem je seznam popisující všechna plánovaná a existující ochranná opatření (2).
- Výběr ochranných opatření – ochranná opatření se využívají k minimalizaci případných rizik. Jednotlivá opatření a jejich cíle jsou popsána v normě ISO/IEC 27001 a podrobnější popis lze najít v normě ISO/IEC 27002 (2).
- Odhad rizik – v tomto kroku se identifikují a odhadují rizika, kterými jsou aktiva vystavena. Je potřeba zjistit, co hrozí a proč to hrozí (2).
- Přijetí rizik – po předchozích krocích nám vždy zůstanou zbytková rizika. Nikde nelze vytvořit úplně bezpečný systém a v reálném provozu se mu můžeme pouze limitně přiblížit. Zbytková rizika se dělí na akceptovatelná a neakceptovatelná. Akceptace rizik může být vybrána z důvodu, že se jedná o nízké riziko nebo

z důvodu, kdy náklady na opatření rizika jsou pro organizaci cenově neúnosné. Pokud riziko nechceme akceptovat, musí proběhnout opětovný výběr ochranných opatření a odhad rizika (3).

- Politika bezpečnosti systému IT – tato část by měla obsahovat souhrn požadovaných ochranných opatření a popis důvodu, proč jsou nezbytná a zavedená (3).
- Plán bezpečnosti IT - souhrnný dokument, ve kterém jsou popsány veškeré akce, které musí být uskutečněny, aby mohla být ochranná opatření aplikována (3).

2.7 Obecné nařízení o ochraně osobních údajů

Obecné nařízení o ochraně osobních údajů (anglicky – General Data Protection Regulation, zkratkou GDPR) Evropského parlamentu a Rady EU č. 2016/679 nabývá účinnosti dne 25. května 2018 a platí pro všechny organizace nabízející služby a zboží v rámci EU a manipulující s osobními údaji fyzických osob. Protože se jedná o nařízení, představuje na rozdíl od směrnice Evropské unie přímo účinný právní předpis, to znamená, že k jeho účinnosti jej není třeba zavádět českou právní úpravou (má přednost před národní legislativou). Na nařízení právně navazuje národní právní úprava, kterou v České republice představuje zákon č.101/2000 Sb., o ochraně osobních údajů (v současné době se připravuje novelizace tohoto zákona tak, aby odpovídal obecnému nařízení o ochraně osobních údajů). Nařízení zpřesňuje ochranu osobních údajů a posiluje právo fyzické osoby na kontrolu zpracování osobních údajů (hlavně výší sankcí pro nedodržování nařízení). GDPR se týká všech osobních údajů, které jsou například zachyceny v listinné podobě nebo elektronické podobě, zejména pak v informačních systémech. Pro obce je také typická jejich role zřizovatele dalších právnických osob (neziskových organizací, školských právnických osob, akciové společnosti, atd.). Je tedy povinností obce, aby zajistila poučení o povinnostech v oblasti ochrany osobních údajů a implementaci odpovídajících procesů též u těchto subjektů (20).

Podle Úřadu pro ochranu osobních údajů vznikají při zpracování osobních údajů tyto nové povinnosti (21):

- posouzení vlivu na ochranu osobních údajů (DPIA),
- povinnost vést záznamy o činnostech zpracování údajů,

- ohlašování případů porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů,
- předchozí konzultace s dozorovým úřadem,
- jmenování pověřence pro ochranu osobních údajů.

2.7.1 Osobní údaj

Osobními údaji se rozumí všechny informace o identifikované nebo identifikovatelné fyzické osobě. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat za pomocí identifikátoru, nebo díky jednomu či více zvláštních prvků fyzické, fyziologické, psychické, genetické, ekonomické, kulturní nebo společenské identity této fyzické osoby (20).

Za osobní údaje lze například považovat: jméno, příjmení, pohlaví, IP adresu, fotografii, věk, datum narození, občanství, stav, rodné číslo, emailovou adresu, telefonní číslo, adresu bydliště, adresu pracoviště, síťové identifikátory, atd. Do zvláštní kategorie osobních údajů lze zařadit například: etnický a rasový původ, zdravotní stav, náboženské vyznání, tresty a odsouzení, sexuální orientaci, politické názory, členství v odborových organizacích, osobní údaje dětí, genetické informace, biometrické informace, ekonomickou identitu, atd. (20).

2.7.2 Zpracování osobních údajů

Za zpracování osobních údajů se považuje jakákoli operace nebo soubor operací s osobními údaji, který je prováděn pomocí nebo bez pomoci autorizovaných postupů. Za typické zpracování údajů se bere: shromažďování dat, zaznamenávání dat, uspořádání dat, strukturování dat, uložení dat, přizpůsobení nebo pozměnění dat, vyhledávání dat, nahlédnutí na data, použití dat, zpřístupnění dat přenosem, šíření dat nebo jakékoliv zpřístupnění, seřazení nebo zkombinování dat, omezení dat, výmaz nebo zničení dat. Dále také zpracování osobních údajů podle obecného nařízení dopadá, jak na zpracování osobních údajů ve společnosti správce nebo zpracovatele, tak i na zpracování osobních údajů v cloudu nebo v cloudových službách (20).

2.7.3 Správce

Fyzická nebo právnická osoba, která sama nebo spolu s jinými určuje účel a způsoby zpracování osobních údajů, případně ten, kdo je určen jako správce zákonem. Mezi povinnosti správce ukládané obecným nařízením o ochraně osobních údajů patří například (20):

- zajistit, že zpracování osobních údajů bude odpovídat nařízení a zavést vhodná organizační a technická opatření,
- zajistit zabezpečení zpracování osobních údajů,
- zajistit provádění posouzení vlivu na ochranu osobních údajů,
- zajistit, aby se včas ohlašovala porušení bezpečnosti osobních údajů,
- vedení záznamů o činnostech zpracování osobních údajů,
- zajistit pouze takové zpracovatele, kteří jsou schopni splnit zpracování dle nařízení,
- správce musí být schopen předložit implementovaná opatření.

2.7.4 Zpracovatel

Fyzická nebo právnická osoba, která zpracovává osobní údaje jménem správce. Zpracovatel a správce musí mít smluvní vztah, ve kterém je obsaženo: účel a doba trvání zpracování osobních údajů, předmět zpracování, typy osobních údajů a kategorie subjektu údajů, práva a povinnosti správce (20).

2.7.5 Zákonnost zpracování osobních údajů

Musí být splněna minimálně jedna z podmínek (20):

- souhlas nebo smlouva se subjektem,
- zpracování je nezbytné pro plnění smlouvy,
- veřejný zájem nebo oprávněné zájmy správce,
- zákonné činnosti,
- životně důležité zájmy subjektů dat.

Souhlas subjektu musí být svobodný, konkrétní, informovaný a jednoznačný.

2.7.6 Práva subjektů osobních údajů

Před udělením souhlasu fyzické osoby se zpracováním jejích osobních údajů musí být osoba poučena o tom, že má právo po správci nebo zpracovateli požadovat (20):

- přístup k osobním údajům,
- opravu nebo výmaz („právo být zapomenut“),
- omezení zpracování jednotlivých osobních údajů,
- omezení přenositelnosti údajů,
- vznesení námitky.

Toto se vztahuje na všechny osobních údaje fyzické osoby včetně nestrukturovaných dat uložených například v přílohách emailů nebo na uložištích (20).

2.7.7 Pověřená osoba pro ochranu osobních údajů

Pověřenec (DPO - data protecion officer) má za úkol monitorování souladu zpracování osobních údajů s povinnostmi vyplývajícími z nařízení, provádění interních auditů, školení pracovníků a celkové řízení agendy interní ochrany dat. Povinně musí funkci DPO zřídit (vlastním zaměstnancem nebo externí osobou) orgány veřejné moci (obce, školy), ten kdo provádí rozsáhlé systematické monitorování fyzických osob, ten kdo zpracovává zvláštní kategorie osobních údajů (banky, nemocnice (20)).

2.7.8 Posuzování vlivu na ochranu osobních údajů

Novou změnou v GDPR je také povinnost posuzování vlivu na ochranu osobních údajů (DPIA - Data Protection Impact Assessment). Posuzování vlivu provádí správce v případě (podle článku 35 odst. 1 GDPR), kdy určitý druh zpracování údajů bude mít pravděpodobně za následek vysoké riziko pro práva a svobody fyzických osob, a to hlavně při využívání nových technologií.

3 ANALÝZA SOUČASNÉHO STAVU BEZPEČNOSTI

V této části diplomové práce je analyzován současný stav informační bezpečnosti v obci, na základě kterého se v další části práce vytvoří soubor doporučení dle ISMS pro zvýšení informační bezpečnosti.

3.1 Představení organizace

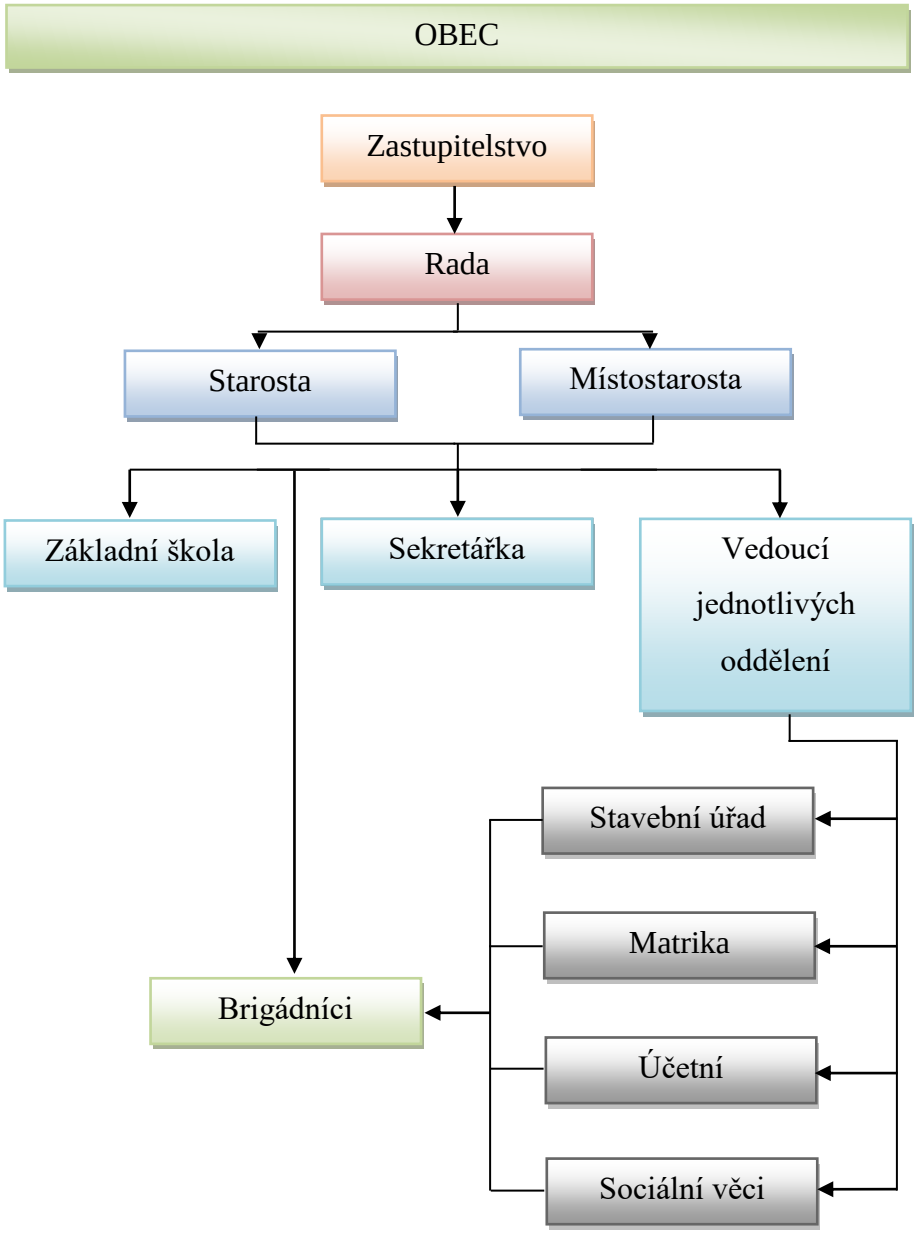
Z důvodu bezpečnosti informací organizace, v této práci nebude uváděn přesný název nebo jakákoli informace, která by vedla k její identifikaci.

Podle rozdělení obcí právní legislativou se jedná o běžný obecní úřad, který vykonává základní rozsah samosprávy a jde o obec označovanou jako „jednotková“ či obec I. stupně. V čele úřadu stojí starosta, který se stará o chod organizace. Úřad se ve své činnosti řídí podle zákona 128/2000 Sb., zákon o obcích (obecní zřízení), v platném znění. V určitých činnostech vykonává tzv. samosprávu, která je v zájmu obce a její občanů. Dále se řídí upravenými zákony, které na úřad přenáší určitá práva a povinnosti. Úřad musí plnit úkoly přijaté od starosty, místostarosty, zastupitelstva, rady a může rozhodovat v případech stanovených zákonem o obcích nebo zvláštním zákonem.

Pod svou správou má dále také tři tzv. “části obce“, které jsou od hlavní obce katastrálně odděleny. Za tyto obce vykonává všechny řídící činnosti.

3.2 Organizační struktura obce

Z důvodu, že obec právně spadá pod stát, je organizační struktura jasně daná a liší se maximálně v koncových pozicích. Počty zaměstnanců se odvíjí od počtu obyvatel a rozpočtu obce. Na obecním úřadě pracuje celkem 15 zaměstnanců na plný úvazek včetně starosty, dále potom místostarosta a členové zastupitelstva na smluvený počet hodin týdně a mzdu. Starosta se stará o celkové vedení úřadu a spadají pod něj všichni zaměstnanci a úkoly organizace. Místostarosta se stará o plánování změn územního plánu, životní prostředí a sociální věci. Organizační strukturu obecního úřadu lze vidět na Obrázku **9**.



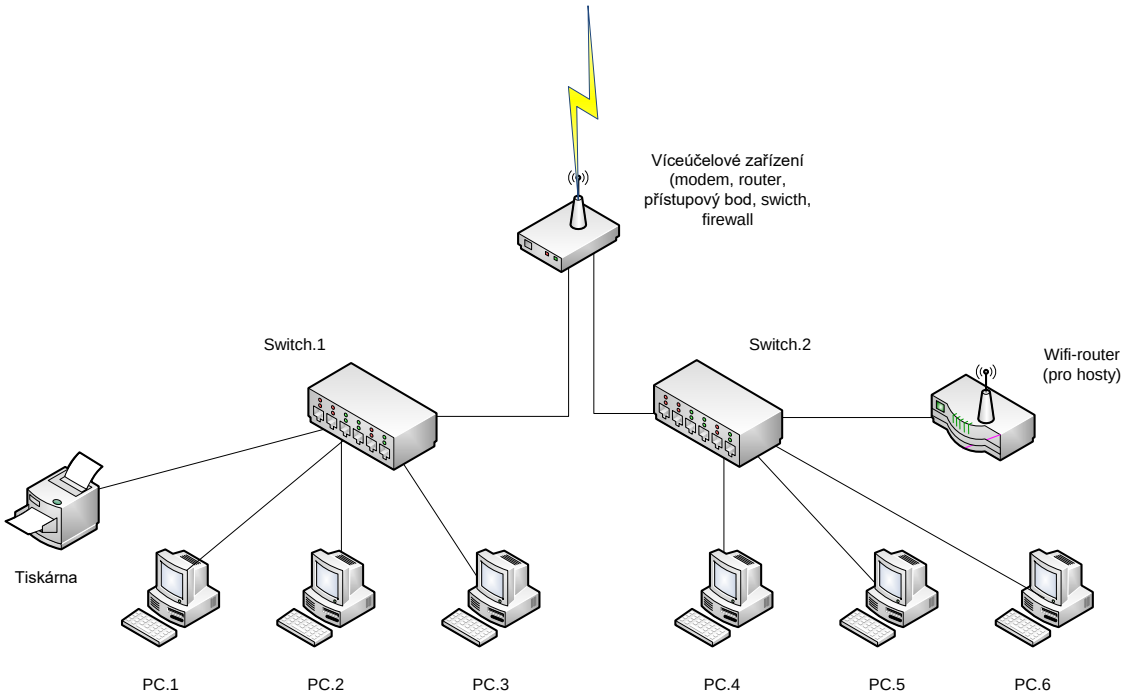
Obrázek 9: Organizační struktura Obce. Zdroj: vlastní zpracování

Dále jsou v organizaci zaměstnáváni brigádníci, kteří vypomáhají stálým zaměstnancům v jejich běžné činnosti na úřadě a vykonávají veřejně prospěšné práce. Všichni zaměstnanci při nástupu na své pozice podepisují pracovní smlouvu, v níž se mimo jiné zavazují k mlčenlivosti k citlivým informacím a pracovních postupů obecního úřadu.

O provoz ICT se stará primárně starosta, který má v tomto oboru vystudovanou vysokou školu. Stará se tedy o základní problémy, které se dají vyřešit jednoduše a rychle. Na složitější problémy a celkovou údržbu má obecní úřad najatou IT firmu z nedalekého města. Tato firma se stará o servis počítačů, obměnu slabších a starších komponentů, instalace softwarů přes vzdálenou plochu a o jakékoli problémy, které nedokáže vyřešit sám starosta.

3.3 Analýza ICT organizace

Obecní úřad ke své činnosti využívá 13 počítačů připojených do sítě, z čehož jsou 3 notebooky, které se využívají na práci v terénu. Pracovní stanice mají všichni stálí zaměstnanci kromě uklízeček a sociální pracovnice. Všechny nepřenosné pracovní stanice jsou připojeny do sítě pomocí LAN adaptéru a notebooky pomocí Wi-Fi. LAN síť je vytvořena kabelovými rozvody prostřednictvím UTP kabelů Cat.6 položených do plastových DIN lišt upevněných na zdech, které končí v jednotlivých kancelářích zásuvkami RJ-45. Budova je pomyslně rozdělena na dvě části a pro každou z nich slouží samostatný switch, přes který se připojují jednotlivé kanceláře. Tyto switche jsou napojeny na víceúčelové zařízení (modem, router, switch, přístupový bod, firewall), který je umístěn v kanceláři starosty, kde se nachází i zálohovací pevné disky, do kterých pravidelně dvakrát týdně starosta ukládá zálohy ze všech pracovních stanic zaměstnanců. Pevné disky jsou uloženy v trezoru starosty. Wi-Fi sítě jsou zde nainstalované dvě. Jedna veřejná pro hosty úřadu se zabezpečením WPA2-AES (Wi-Fi Protected Access II - Advenced Encryption Standard) s heslem zjistitelným od sekretářky a druhá pro zaměstnance se stejným zabezpečením WPA2-AES. Logické řešení sítě lze vidět na Obrázku **10**.



Obrázek 10: Logické řešení sítě. Zdroj: vlastní zpracování

3.3.1 Hardware

Harware jednotlivých kanceláří úřadu je tvořen různými PC sestavami, v kterých jsou jednou za dva roky obměňovány komponenty a jednou za čtyři roky jsou měněny zcela. Každá pracovní stanice je napojena do elektrické sítě přes zdroj nepřerušovaného napětí (UPS), aby v případě výpadku elektrické sítě nedocházelo k zbytečným ztrátám či poškozením dat a poškození pracovních stanic.

Dále budou popsány hlavní pracovní stanice v jednotlivých kancelářích (v některých kancelářích se jich nachází více, ale většinou nejsou tak výkonné nebo používané jako ty, co budu popisovat).

V kanceláři starosty se nachází PC sestava HAL3000 Gold s platformou AMD, která je osazena procesorem AMD RYZEN R5 1600 3,2 GHz, základní deskou MSI B350 PC MATE, operační pamětí 8GB DDR4, grafickou kartou GeForce GTX 1060 6GB a pevným diskem Seagate 1TB Barracuda.

Na matrice se nachází PC sestava HAL3000 Bronze 9204P s procesor INTEL Pentium G840 2,8GHz, základní deskou IntelH61/ LGA1155/ DDR3, operační pamětí 2 x KINGMAX RAM DDR3 2GB, grafickou kartou INTEL HD graphics a pevným diskem 500GB HDD SATA300.

Vedoucí stavebního úřadu pracuje na sestavě HAL3000 Easywork, která je osazena procesorem INTEL Pentium G3240 3,1GHz, grafickou kartou INTEL HD graphics, operační pamětí 4GB a pevným diskem 500GB.

V kanceláři účetní se nachází PC sestava HAL3000 EliteWork III s procesorem Intel Core i5-7400, základní deskou MSI H110M ECO, operační pamětí ADATA 8GB DDR4 2400MHz, grafickou kartou Intel HD Graphics a pevným diskem Seagate Barracuda 1TB.

Sekretářka používá sestavu Fujitsu Esprimo P2560 s procesorem Intel Core 2 Duo, základní deskou D3041 provedení µATX, operační pamětí 2x 2 GB DDR3 1066MHz, grafickou kartou INTEL GMA 4500 a pevným diskem HDD 500GB .

Místostarosta ke své práci využívá sestavu HP ProDesk 400 G1 SFF s procesorem Intel Core i3 4160, základní deskou Intel 1150, operační pamětí 4GB DDR3, grafickou kartou Intel HD Graphics 4400 a pevným diskem Seagate Barracuda 1TB

3.3.2 Software

Operační systém

Všechny pracovní stanice jsou vybaveny stejným operačním systémem Microsoft Windows 10 Professional, ve kterém je nainstalovaný kancelářský balík Microsoft Office 2013.

Informační systém

Obec má zakoupený licencovaný informační systém GINIS od společnosti Gordic s výběrem určitých modulů. Tento informační systém se nachází pouze na třech pracovních stanicích a to tam, kde se denně využívá (matrika, účetní, starosta). Obec má zaplacené tyto moduly: pokladna, matrika, registr obyvatel, daně, dávky, pohledávky. V této době je nainstalován na třech počítačích, a také se tam data z modulů ukládají, avšak v dohledné době se bude přecházet na cloudovou verzi z důvodu lepšího zabezpečení informací a nastupující GDPR.

Antivir

Proti škodlivým programům je na každé pracovní stanici nainstalován antivir NOD 32 a dále každý operační systém obsahuje vestavěný firewall od Microsoftu.

Ostatní software

Systém ASPI

ASPI je automatizovaný systém pro práci s právními informacemi. Obsahuje všechny právní předpisy vydané na území ČR a také předpisy Evropské unie a Evropského společenství. Obec tento systém používá při dohledávání zákonů či vyhlášek. Nově se v tomto systému nachází i praktické nástroje k GDPR.

Program Domovník

Obec tento program využívá na vedení záznamu o domech, bytech, nájemnících a také revizích, platbách, vyúčtování a evidenci dokumentů. U bytů lze také mimo údaje o lidech vést záznamy o topných tělesech, plochách místností, vybavení a také slevách.

Pinnacle Studio

V tomto softwaru obec stříhá a upravuje videa z místních akcí a zastupitelských porad.

3.4 Umístění objektu

Budova obecního úřadu je umístěna uprostřed obce na hlavním náměstí. Součástí náměstí je nehlídané parkoviště, které je určeno pro zaměstnance a návštěvníky úřadu. Uvnitř budovy je jedno poschodí, přízemí a sklep. Ve sklepě je umístěna kotelna, rozvod vody a plynu, dílna a místnost zařízená pro údržbáře objektu a obecního majetku. V přízemí jsou kromě vstupní chodby a schodů tři místnosti. V první se nachází archiv všech papírových spisů a obecní rozhlas. Druhá a třetí slouží k zasedání zastupitelstva, významným událostem a oslavám. V poschodí se nachází všechny kanceláře zaměstnanců úřadu. Kancelář starosty, kde jsou uloženy téměř všechny aktivní prvky a zálohovací disky, je přístupná pouze přes kancelář sekretářky úřadu.

3.4.1 Zabezpečení budovy

Do budovy se lze dostat pouze jedním vchodem, a to hlavními dveřmi. Tyto dveře jsou chráněny dvěma zámky, vnitřním pohybovým čidlem alarmu, který je napojen na bezpečnostní firmu, a venkovní kamerou. Hned za vchodovými dveřmi se nachází předsíň zakončená dalšími dveřmi. Tyto dveře jsou v úředních hodinách otevřené. Mimo úřední hodiny si zaměstnanci dveře otevírají klíčem a hostům je otevírá sekretářka úřadu na zavolání. Uvnitř budovy je kamerový systém, který pořizuje záznam v době pohybu na dané kameře a doba uchování je 3 měsíce. Přístup do starostovy kanceláře je možný pouze přes kancelář sekretářky úřadu. Ostatní kanceláře jsou pak zabezpečené obyčejnými dveřními zámky. Každý zaměstnanec má pracovní stůl se zamykatelnými šuplíky, do kterých je povinný na konci pracovní doby zamknout všechny důležité dokumenty a jakékoli přenosné úložné disky.

3.5 Analýza rizik

V této části práce budou analyzována a ohodnocena rizika organizace. Z analýzy rizik vychází výsledný návrh, díky němuž se redukují nebo úplně vylučují zjištěná rizika. Tomuto kroku předchází identifikace aktiv a ohodnocení aktiv. Na základě identifikace aktiv a analýzy hrozeb je sestavena matice zranitelnosti a matice rizik. Následně v další kapitole jsou zavedena opatření k eliminaci identifikovaných rizik. Analýza rizik je vypracovaná v souladu s metodikou normy ČSN ISO/IEC 27005:2013, která se zabývá řízením rizik bezpečnosti informací a obsahuje návod na identifikaci hrozeb, zranitelností, matici zranitelností a rizika.

3.5.1 Identifikace a hodnocení aktiv

Aby se dalo provést ohodnocení aktiv je nutné aktiva nejdříve idenfitikovat. Identifikace byla prováděna společně s vedením organizace. Všechna aktiva, která byla identifikována, mají velký vliv na zajištění plnohodnotného chodu organizace. Aktiva jsou ohodnocena na stupnici od 1 do 5. Význam ohodnocení lze vidět v Tabulce **1**.

Tabulka 1: Hodnocení aktiv. Zdroj: vlastní zpracování

Klasifikační stupeň	Dopad rizika na organizaci	Riziko
1	Žádný dopad	Bezvýznamné
2	Zanedbatelný dopad	Akceptovatelné
3	Potíže nebo finanční ztráty	Nízké
4	Vážné potíže či podstatné finanční ztráty	Nežádoucí
5	Existenční potíže	Nepřijatelné

V druhé tabulce jsou uvedena identifikovaná aktiva, která jsou nejdůležitější z pohledu společnosti. U aktiv byl hodnocen dopad na integritu, důvěrnost a dostupnost. Výpočet celkové hodnoty aktiva probíhal pomocí tzv. součtového algoritmu. Princip tohoto algoritmu je takový, že se sečtou všechny tři proměnné a poté se vydělí jejich počtem.

$$\text{Celková hodnota aktiva} = (\text{Dostupnost} + \text{Důvěrnost} + \text{Integrita}) \,/\, 3$$

V Tabulce 2 můžeme vidět, že jsou pro obec nejdůležitější aktiva: archiv, osobní údaje, operační systém, informační systém, zálohy dat a interní spisový materiál.

Tabulka 2: Identifikace aktiv a jejich ohodnocení. Zdroj: vlastní zpracování

Typ aktiva	Aktivum	Dostupnost	Důvěrnost	Integrita	Váha
Hardware	Pracovní stanice	3	3	3	3
	Přenosné uložiště	3	4	2	3
	Tiskárna	3	4	2	3
	ICT infrastruktura	4	3	3	3
Software	Operační systém	4	5	3	4
	Informační systém	3	5	4	4
	Programové vybavení	2	3	3	3
Data	Osobní údaje	5	5	4	5
	Zálohy dat	4	5	3	4
Služby	Připojení k internetu	2	1	2	2
	Fax	1	4	2	2
Další	Kamerový systém	3	3	3	3
	Archiv	5	5	5	5
	Interní spisový materiál	5	4	5	5
	Interní směrnice a předpisy	2	3	3	3

3.5.2 Identifikace zranitelností a hrozeb

Aby šla sestavit matice zranitelnosti, je potřeba nejdříve identifikovat hrozby, u kterých se určí pravděpodobnost, s jakou se mohou vyskytnout. Pravděpodobnosti výskytu hrozeb jsou v Tabulce 3.

Tabulka 3: Ohodnocení hrozeb. Zdroj: vlastní zpracování

Hodnota	Význam hrozby	Slovní vyjádření
1	Velmi nepravděpodobný	Bezvýznamné riziko
2	Málo pravděpodobný	Přijatelné riziko
3	Pravděpodobný	Nepatrné riziko
4	Velmi pravděpodobný	Nežádoucí riziko
5	Téměř jistý	Nepřijatelné riziko

Po vytvoření stupnice pravděpodobností je třeba vybrat hrozby, které mohou ohrozit aktiva společnosti a tím i omezit samotný chod společnosti. V Tabulce 4 jsou vybrány identifikované hrozby z normy ČSN ISO/IEC 27005:2013 a doporučení od vedení obce.

Tabulka 4: Pravděpodobnost výskytu konkrétních hrozeb. Zdroj: vlastní zpracování

	Hrozba	Pravděpodobnost
Fyzické poškození	Poškození požárem	2
	Poškození vodou	1
	Úder blesku	2
Technické problémy	Selhání pracovních stanic	3
	Selhání síťových prvků	2
	Zanedbaná údržba/úklid	2
Výpadek služeb	Výpadek elektřiny	3
	Výpadek internetu	2
	Výpadek webových služeb	1
Nezákonná činnost	Napadení virem	3
	Napadení hackerem	3
	Neoprávněný přístup do sítě	2
	Záměrná škodlivá činnost	2
	Neoprávněné kopírování dat	2
Pochybení zaměstnanců	Vyzrazení přístupových hesel	3
	Vyzrazení citlivých informací	2
	Porušení mlčenlivosti	4
Ohrožení důvěrnosti	Krádež médií nebo dokumentů	2
	Špatné zabezpečení sítě	3
	Špatné zabezpečení budovy	3
	Špatně nastavené přístupové práva	1

3.5.3 Matice zranitelnosti

Matice obsahuje aktiva a hrozby z předchozích tabulek, kde stanovuje úroveň zranitelnosti mezi hrozbou a aktivem. Hrozba nemusí vždy ovlivňovat aktiva velkou mírou (tento fakt lze vidět v kolonkách, kde se nacházejí jedničky). Stupnice zranitelnosti může nabývat hodnot od 1 do 5 (čím větší zranitelnosti, tím vyšší číslo). Sestavení matice je vyobrazeno v Tabulce **5**.

Tabulka 5: Matice zranitelnosti. Zdroj: vlastní zpracování

Tabulka zranitelnosti	*Pravděpodobnost*	**Aktiva**	Pracovní stanice	Přenosné uložiště	Tiskárna	ICT infrastruktura	Operační systém	Informační systém	Programové vybavení	Osobní údaje	Zálohy dat	Připojení k internetu	Fax	Kamerový systém	Archiv	Interní spisový materiál	Interní směrnice a předpisy
Hodnota aktiva			3	3	3	3	4	4	3	5	4	2	2	3	5	5	3
Hrozba																	
Poškození požárem	2		5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
Poškození vodou	1		3	2	4	4	3	3	3	3	2	4	3	2	4	4	3
Úder blesku	2		4	1	4	4	1	1	1	1	1	4	4	3	1	1	1
Selhání pracovních stanic	3		3	1	1	1	1	1	1	1	1	1	1	2	1	1	1
Selhání síťových prvků	2		1	1	3	5	2	2	2	1	1	5	1	1	1	1	1
Zanedbaná údržba/úklid	2		4	2	2	2	1	1	1	1	3	2	2	2	3	2	1
Výpadek elektřiny	3		5	1	5	5	1	1	1	1	1	5	5	5	1	1	1
Výpadek internetu	2		3	1	1	3	2	2	2	1	1	5	1	1	1	1	1
Výpadek webových služeb	1		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Napadení virem	3		4	4	2	3	3	3	3	2	3	3	1	3	1	1	1
Napadení hackerem	3		2	2	2	3	3	3	3	4	1	3	1	3	1	1	1
Neoprávněný přístup do sítě	2		3	2	3	3	2	2	2	4	1	3	1	3	1	1	1
Záměrná škodlivá činnost	2		4	3	3	4	2	2	2	3	3	3	2	2	3	3	3
Neoprávněné kopírování dat	2		1	1	1	1	1	1	1	4	1	1	2	1	1	3	1
Vyzrazení přístupových hesel	3		4	1	1	3	3	2	2	3	1	3	2	2	1	1	1
Vyzrazení citlivých informací	2		1	1	1	1	1	1	1	5	1	1	1	1	1	3	1
Porušení mlčenlivosti	4		1	1	1	1	1	1	1	5	1	1	1	1	1	3	3
Krádež médií nebo dokumentů	2		3	5	2	2	1	1	1	4	5	2	1	1	5	4	3
Špatné zabezpečení sítě	3		3	1	2	4	1	2	2	3	1	3	1	2	1	1	1
Špatné zabezpečení budovy	3		3	3	3	3	1	1	1	2	4	2	2	3	4	4	4
Špatně nastavené přístupové práva	1		1	1	1	3	3	3	3	1	1	3	1	1	1	1	1

3.5.4 Matice rizik

Matice rizik se sestavuje na základě kombinace hrozeb a aktiv. Pro výpočet míry rizika je používána maticová metoda se třemi parametry. Vzorec tedy vypadá takto:

$$R = T * A * V$$

$$T - hrozba$$

$$A - aktivum$$

$$V - zranitelnost$$

Před samotným sestavováním matice rizik je nutné stanovit hranice rizik, podle kterých bude určována závažnost jednotlivých rizik (Tabulka **6**). Míru rizik jsem rozdělil do pěti skupin na:

- Bezvýznamné – Riziko s téměř nulovou pravděpodobnoostí a dopadem.
- Přijatelné – Riziko s velmi malým dopadem i pravděpodobností.
- Nepatrné – Riziko, které může nastat, ale pro společnost by nemělo mít velký dopad.
- Nežádoucí – Riziko, které má velký vliv na chod společnosti.
- Nepřijatelné – Míra rizika je tak velká, že pokud by nastalo, mělo by vliv na existenci společnosti.

Tabulka 6: Stanovení hranic rizika. Zdroj: vlastní zpracování

Hranice	Míra rizika
0 - 10	Bezvýznamné riziko
11-20	Přijatelné riziko
21-30	Nepatrné riziko
31-60	Nežádoucí riziko
61 a více	Nepřijatelné riziko

Po stanovení hranic rizik již lze sestavit matici, která jde vidět v Tabulce 7.

Tabulka 7: Matice rizik. Zdroj: vlastní zpracování

Tabulka zranitelnosti	*Pravděpodobnost*	**Aktiva**	Pracovní stanice	Přenosné uložiště	Tiskárna	ICT infrastruktura	Operační systém	Informační systém	Programové vybavení	Osobní údaje	Zálohy dat	Připojení k internetu	Fax	Kamerový systém	Archiv	Interní spisový materiál	Interní směrnice a předpisy
Hodnota aktiva			3	3	3	3	4	4	3	5	4	2	2	3	5	5	3
Hrozba																	
Poškození požárem	2		30	30	30	30	40	40	30	50	40	20	20	30	50	50	30
Poškození vodou	1		9	6	12	12	12	12	9	15	8	8	6	6	20	20	9
Úder blesku	2		24	6	24	24	8	8	6	10	8	16	16	18	10	10	6
Selhání pracovních stanic	3		27	9	9	9	12	12	9	15	12	6	6	18	15	15	9
Selhání síťových prvků	2		6	6	18	30	16	16	12	10	8	20	4	6	10	10	6
Zanedbaná údržba/úklid	2		24	12	12	12	8	8	6	10	24	8	8	12	30	20	6
Výpadek elektřiny	3		45	9	45	45	12	12	9	15	12	30	30	45	15	15	9
Výpadek internetu	2		18	6	6	18	16	16	12	10	8	20	4	6	10	10	6
Výpadek webových služeb	1		3	3	3	3	4	4	3	5	4	2	2	3	5	5	3
Napadení virem	3		36	36	18	27	36	36	27	30	36	18	6	27	15	15	9
Napadení hackerem	3		18	18	18	27	36	36	27	60	12	18	6	27	15	15	9
Neoprávněný přístup do sítě	2		18	12	18	18	16	16	12	40	8	12	4	18	10	10	6
Záměrná škodlivá činnost	2		24	18	18	24	16	16	12	30	24	12	8	12	30	30	18
Neoprávněné kopírování dat	2		6	6	6	6	8	8	6	40	8	4	8	6	10	30	6
Vyzrazení přístupových hesel	3		36	9	9	27	36	24	18	45	12	18	12	18	15	15	9
Vyzrazení citlivých informací	2		6	6	6	6	8	8	6	50	8	4	4	6	10	30	6
Porušení mlčenlivosti	4		12	12	12	12	16	16	12	100	16	8	8	12	20	60	36
Krádež médií nebo dokumentů	2		18	30	12	12	8	8	6	40	40	8	4	6	50	40	18
Špatné zabezpečení sítě	3		27	9	18	36	12	24	18	45	12	18	6	18	15	15	9
Špatné zabezpečení budovy	3		27	27	27	27	12	12	9	30	48	12	12	27	60	60	36
Špatně nastavené přístupové práva	1		3	3	3	9	12	12	9	5	4	6	2	3	5	5	3
Součet hodnot			417	273	324	414	344	344	258	655	352	268	176	324	420	480	249

3.5.5 Vyhodnocení analýzy rizik

Ve výsledné matici rizik lze vidět, že nejvíce ohrožená aktiva jsou Osobní údaje, Interní spisový materiál a Archiv. U těchto tří aktiv můžeme říci, že to jsou hlavní nositelé informací o organizaci, klientech, občanech nebo samotném státě. Z jakéhokoli pochybení při práci s těmito daty, jejich ztrátě nebo poškození by mohly vznikat situace ohružující chod organizace a dále také finanční či právní spory. Z tohoto důvodu nesmí obec na jejich zabezpečení šetřit a měla by docílit nejvyššího stupně jejich zabezpečení. Návrh opatření na zjištěná rizika je v Kapitole 3.

3.5.6 Zabezpečení nejvíce ohrožených aktiv

Nejvíce ohrožená aktiva Osobní údaje, Interní spisový materiál a Archiv můžeme nazývat jako dokumenty obsahující citlivé informace. Ochranu těchto dokumentů můžeme rozdělit do tří skupin: IT zabezpečení dokumentů, fyzické zabezpečení dokumentů, personální zabezpečení dokumentů.

IT zabezpečení dokumentů

Informace uchovávané elektronicky jsou uloženy vždy v počítači zaměstnance, který je ke své práci potřebuje. Zálohovány jsou pak na přenosných pevných discích v kanceláři starosty. Někteří zaměstnanci si ukládají data na přenosné disky, které jsou pak zamčeny v pracovních stolech. Každý zaměstnanec má svůj počítač s osobním účtem. Osobní účet je chráněn heslem, které zná pouze zaměstnanec, jenž na počítači pracuje. Svoje heslo si musí chránit před zneužitím a jeho ztrátu musí ihned hlásit starostovi, který přes administrátorský účet daného počítače heslo změní.

Fyzické zabezpečení dokumentů

Papírové dokumenty jsou uloženy v jednotlivých kancelářích zaměstnanců a v archivu. Do kanceláří má přístup kompetentní zaměstnanec, uklízečka, starosta a jiní zaměstnanci, kteří mohou požádat v nepřítomnosti daného zaměstnance o klíče pro vstup. Archiv, nacházející se v přízemí budovy obecního úřadu, má na oknech nainstalované mříže a klíče k přístupovým dveřím mají všichni zaměstnanci, kteří s dokumenty archivu pracují.

Personální zabezpečení dokumentů

Každý zaměstnanec při nástupu na pracovní pozici podepisuje smlouvu, díky níž je vázan mlčenlivostí. Všichni jsou důkladně proškoleni, aby věděli jaké informace mohou při vykonávání své agendy sdělovat klientům či jiným osobám.

4 VLASTNÍ NÁVRHY

V této části práce bude vytvořen soubor bezpečnostních opatření pro minimalizaci rizik obce. Opatření budou vytvářena na základě rizik, která byla identifikována v matici zranitelnosti a matici rizik v analytické části práce. Tato navržená bezpečnostní opatření jsou vytvářena podle normy ČSN ISO/IEC 27001:2014 a při jejich aplikaci bylo vycházeno z doporučení normy ČSN ISO/IEC 27002:2014. Organizace v blízké době neplánuje usilovat o certifikaci ISMS, jak z důvodu finančního, tak z důvodu konání komunálních voleb do zastupitelstva obce, které by změnou zastupitelstva mohly ohrozit její zavádění. V této kapitole tedy navrhnu k zavedení ta opatření, která jsou potřeba zavést přednostně v první etapě, aby tak byla pokryta největší rizika.

Za zavádění bezpečnostních opatření bude zodpovědný starosta obce a v jeho nepřítomnosti místostarosta. Pokud budou do vedení obce v průběhu zavádění ISMS zvoleni jiní lidé (viz podzimní komunální volby), kteří této problematice nerozumí nebo se jí nebudou chtít věnovat, bude nutné najmout externistu.

4.1 Soubor opatření podle ČSN ISO/IEC 27001:2014

Tabulka 8 obsahuje soubor opatření podle ČSN ISO/IEC 27001:2014, ve kterém jsou určeny opatření k zavedení.

Tabulka 8: Soubor opatření dle ISO/IEC 27001. Zdroj: (7)

Označení	Opatření	Situace
A.5	**Politiky bezpečnosti informací**	
A.5.1	**Směřování bezpečnosti informací vedením organizace**	
A.5.1.1	Politiky pro bezpečnost informací	aplikovat
A.5.1.2	Přezkoumání politik pro bezpečnost informací	aplikovat
A.6	**Organizace bezpečnosti informací**	
A.6.1	**Interní organizace**	
A.6.1.1	Role a odpovědnosti bezpečnosti informací	aplikovat
A.6.1.2	Princip oddělení povinností	aplikovat
A.6.1.3	Kontakt s příslušnými orgány a autoritami	aplikováno
A.6.1.4	Kontakt se zájmovými skupinami	neaplikovat

A.6.1.5	Bezpečnost informací v řízení projektů	aplikovat
A.6.2	**Mobilní zařízení a práce na dálku**	
A.6.2.1	Politika mobilních zařízení	aplikovat
A.6.2.2	Práce na dálku	aplikovat
A.7	**Bezpečnost lidských zdrojů**	
A.7.1	**Před vznikem pracovního vztahu**	
A.7.1.1	Prověřování	aplikováno
A.7.1.2	Podmínky pracovního vztahu	aplikováno
A.7.2	**Během pracovního vztahu**	
A.7.2.1	Odpovědnosti vedení organizace	aktualizovat
A.7.2.2	Povědomí, vzdělávání a školení bezpečnosti informací	aplikovat
A.7.2.3	Disciplinární řízení	aktualizovat
A.7.3	**Ukončení a změna pracovního vztahu**	
A.7.3.1	Odpovědnosti při ukončení nebo změně pracovního vztahu	aplikováno
A.8	**Řízení aktiv**	
A.8.1	**Odpovědnost za aktiva**	
A.8.1.1	Seznam aktiv	aktualizovat
A.8.1.2	Vlastnictví aktiv	aktualizovat
A.8.1.3	Přípustné použití aktiv	aktualizovat
A.8.1.4	Navrácení aktiv	aplikováno
A.8.2	**Klasifikace informací**	
A.8.2.1	Klasifikace informací	aplikovat
A.8.2.2	Označování informací	aplikovat
A.8.2.3	Manipulace s aktivy	aplikovat
A.8.3	**Manipulace s médii**	
A.8.3.1	Správa výměnných médií	aplikovat
A.8.3.2	Likvidace médií	aplikovat
A.8.3.3	Přeprava fyzických médií	aplikovat
A.9	**Řízení přístupu**	
A.9.1	**Požadavky organizace na řízení přístupu**	
A.9.1.1	Politika řízení přístupu	aplikovat
A.9.1.2	Přístup k sítím a síťovým službám	aplikovat
A.9.2	**Řízení přístupu uživatelů**	
A.9.2.1	Registrace a zrušení registrace uživatele	aplikováno
A.9.2.2	Správa uživatelských přístupů	aplikováno
A.9.2.3	Správa privilegovaných přístupových práv	aplikovat
A.9.2.4	Správa tajných autentizačních informací uživatelů	aplikovat
A.9.2.5	Přezkoumání přístupových práv uživatelů	aplikovat
A.9.2.6	Odebrání nebo úprava přístupových práv	aplikováno
A.9.3	**Odpovědnosti uživatelů**	
A.9.3.1	Používání tajných autentizačních informací	aplikovat

A.9.4	**Řízení přístupu k systémům a aplikacím**	
A.9.4.1	Omezení přístupu k informacím	aplikovat
A.9.4.2	Bezpečné postupy přihlášení	aplikovat
A.9.4.3	Systém správy hesel	aplikovat
A.9.4.4	Použití privilegovaných programových nástrojů	neaplikovat
A.9.4.5	Řízení přístupu ke zdrojovým kódům programů	neaplikovat
A.10	**Kryptografie**	
A.10.1	**Kryptografická opatření**	
A.10.1.1	Politika pro použití kryptografických opatření	aplikovat
A.10.1.2	Správa klíčů	aplikovat
A.11	**Fyzická bezpečnost a bezpečnost prostředí**	
A.11.1	**Bezpečné oblasti**	
A.11.1.1	Fyzický bezpečnostní perimetr	aktualizovat
A.11.1.2	Fyzické kontroly vstupu	aplikováno
A.11.1.3	Zabezpečení kanceláří, místností a vybavení	aplikováno
A.11.1.4	Ochrana před vnějšími hrozbami a hrozbami prostředí	aplikováno
A.11.1.5	Práce v bezpečných oblastech	neaplikovat
A.11.1.6	Oblasti pro nakládku a vykládku	neaplikovat
A.11.2	**Zařízení**	
A.11.2.1	Umístění zařízení a jeho ochrana	aktualizovat
A.11.2.2	Podpůrné služby	aktualizovat
A.11.2.3	Bezpečnost kabelových rozvodů	aktualizovat
A.11.2.4	Údržba zařízení	aktualizovat
A.11.2.5	Přemístění aktiv	aplikovat
A.11.2.6	Bezpečnost zařízení a aktiv mimo prostory organizace	aplikovat
A.11.2.7	Bezpečná likvidace nebo opakované použití zařízení	aplikovat
A.11.2.8	Uživatelská zařízení bez obsluhy	aplikovat
A.11.2.9	Zásada prázdného stolu a prázdné obrazovky monitoru	aplikovat
A.12	**Bezpečnost provozu**	
A.12.1	**Provozní postupy a odpovědnosti**	
A.12.1.1	Dokumentované provozní postupy	aplikovat
A.12.1.2	Řízení změn	aplikovat
A.12.1.3	Řízení kapacit	aplikovat
A.12.1.4	Princip oddělení prostředí vývoje, testování a provozu	neaplikovat
A.12.2	**Ochrana proti malwaru**	
A.12.2.1	Opatření proti malwaru	aplikováno
A.12.3	**Zálohování**	
A.12.3.1	Zálohování informací	aktualizovat
A.12.4	**Zaznamenávání formou logů a monitorování**	
A.12.4.1	Zaznamenávání událostí formou logů	aplikovat
A.12.4.2	Ochrana logů	aplikovat
A.12.4.3	Logy o činnosti administrátorů a operátorů	aplikovat

A.12.4.4	Synchronizace hodin	aplikovat
A.12.5	**Správa provozního softwaru**	
A.12.5.1	Instalace softwaru na provozní systémy	aplikovat
A.12.6	**Řízení technických zranitelností**	
A.12.6.1	Řízení technických zranitelností	aplikovat
A.12.6.2	Omezení instalace softwaru	aktualizovat
A.12.7	**Hlediska auditu informačních systémů**	
A.12.7.1	Opatření k auditu informačních systémů	neaplikovat
A.13	**Bezpečnost komunikací**	
A.13.1	**Správa bezpečnosti sítě**	
A.13.1.1	Opatření v sítích	aplikovat
A.13.1.2	Bezpečnost síťových služeb	aplikovat
A.13.1.3	Princip oddělení v sítích	aplikovat
A.13.2	**Přenos informací**	
A.13.2.1	Politiky a postupy při přenosu informací	aplikovat
A.13.2.2	Dohody o přenosu informací	aplikovat
A.13.2.3	Elektronické předávání zpráv	aplikovat
A.13.2.4	Dohody o utajení nebo o mlčenlivosti	aplikováno
A.14	**Akvizice, vývoj a údržba systémů**	
A.14.1	**Bezpečnostní požadavky informačních systémů**	
A.14.1.1	Analýza a specifikace požadavků bezpečnost informací	aplikovat
A.14.1.2	Zabezpečení aplikačních služeb ve veřejných sítích	aplikovat
A.14.1.3	Ochrana transakci aplikačních služeb	aplikovat
A.14.2	**Bezpečnost v procesech vývoje a podpory**	
A.14.2.1	Politika bezpečného vývoje	neaplikovat
A.14.2.2	Postupy řízení změn systému	neaplikovat
A.14.2.3	Technické přezkoumání aplikací po změnách provozní platformy	aplikovat
A.14.2.4	Omezení změn softwarových balíků	neaplikovat
A.14.2.5	Principy budování bezpečných systémů	aplikovat
A.14.2.6	Prostředí bezpečného vývoje	neaplikovat
A.14.2.7	Outsourcovaný vývoj	neaplikovat
A.14.2.8	Testování bezpečnosti systémů	neaplikovat
A.14.2.9	Testování akceptace systémů	aplikovat
A.14.3	**Data pro testování**	
A.14.3.1	Ochrana dat pro testování	neaplikovat
A.15	**Dodavatelské vztahy**	
A.15.1	**Bezpečnost informací v dodavatelských vztazích**	
A.15.1.1	Politika bezpečnosti informaci pro dodavatelské vztahy	aplikovat
A.15.1.2	Bezpečnostní požadavky v dohodách s dodavateli	aplikovat
A.15.1.3	Dodavatelský řetězec informačních a komunikačních technologií	aplikovat
A.15.2	**Řízení dodávek služeb dodavatelů**	

A.15.2.1	Monitorování a přezkoumávání služeb dodavatelů	aplikovat
A.15.2.2	Řízení změn ve službách dodavatelů	aplikovat
A.16	**Řízení incidentů bezpečnosti informací**	
A.16.1	**Řízení incidentů bezpečnosti informací a zlepšování**	
A.16.1.1	Odpovědnosti a postupy	aplikovat
A.16.1.2	Hlášení událostí bezpečnosti informací	aktualizovat
A.16.1.3	Hlášení slabých míst bezpečnosti informací	aktualizovat
A.16.1.4	Posouzení a rozhodnutí o událostech bezpečnosti informací	aplikovat
A.16.1.5	Reakce na incidenty bezpečnosti informací	aplikovat
A.16.1.6	Ponaučení z incidentů bezpečnosti informací	aktualizovat
A.16.1.7	Shromažďování důkazů	aplikovat
A.17	**Aspekty řízení kontinuity činností organizace z hlediska bezp. informací**	
A.17.1	**Kontinuita bezpečnosti informací**	
A.17.1.1	Plánování kontinuity bezpečnosti informací	aplikovat
A.17.1.2	Implementace kontinuity bezpečnost informací	aplikovat
A.17.1.3	Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací	aplikovat
A.17.2	**Redundance**	
A.17.2.1	Dostupnost vybavení pro zpracování informací	aplikovat
A.18	**Soulad s požadavky**	
A.18.1	**Soulad s právními a smluvními požadavky**	
A.18.1.1	Identifikace odpovídající legislativy a smluvních požadavků	aplikováno
A.18.1.2	Ochrana duševního vlastnictví	aplikováno
A.18.1.3	Ochrana záznamů	aktualizovat
A.18.1.4	Soukromí a ochrana osobních údajů	aktualizovat
A.18.1.5	Regulace kryptografických opatření	neaplikovat
A.18.2	**Přezkoumání bezpečnosti informací**	
A.18.2.1	Nezávislá přezkoumání bezpečnosti informací	aplikovat
A.18.2.2	Shoda s bezpečnostními politikami a normami	aplikovat
A.18.2.3	Přezkoumání technické shody	neaplikovat

4.2 Plán zavedení opatření

Vzhledem k tomu, že obec není moc veliká, tak nemá zdroje, kterými by mohla všechny opatření zavést v krátkém čase, čímž by mohla usilovat o certifikaci ISMS. Z tohoto důvodu lze zavedení opatření rozdělit do více částí a na delší časové období. Zavádění bezpečnostních opatření jsem tedy rozdělil do dvou etap, z nichž budu zavádět pouze první. Primárně budu zavádět opatření na rizika, která vyšla jako nejvíce závažná z matice rizik a opatření která budou nápomocna při zavádění GDPR. Opatření na rizika se budou provádět akceptací rizika (riziko se přijme a neprovádí se žádné akce) a redukcí rizika (odstranění příčiny vzniku rizika nebo dopad rizika, riziko se přesouvá na další subjekty, provedou se pojištění proti následkům rizika nebo se zavedou opatření ke snížení či úplnému odstranění rizika).

První etapa obsahuje tato opatření:

- A.5 Politiky bezpečnosti informací
- A.6 Organizace bezpečnosti informací
- A.7 Bezpečnost lidských zdrojů
- A.8 Řízení aktiv
- A.9 Řízení přístupu
- A.10 Kryptografie
- A.11 Fyzická bezpečnost a bezpečnost prostředí
- A.12 Bezpečnost provozu

Druhá etapa obsahuje tato opatření:

- A.13 Bezpečnost komunikací
- A.14 Akvizice, vývoj a údržba systémů
- A.15 Dodavatelské vztahy
- A.16 Řízení incidentů bezpečnosti informací
- A.17 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací
- A.18 Soulad s požadavky

4.3 Zavedení bezpečnostních opatření první etapy

V této kapitole budou popsána zaváděná opatření v souladu s doporučením normy ISO/IEC 27002:2014, avšak některá jsou přizpůsobena potřebám organizace.

4.3.1 A.5 Politiky bezpečnosti informací

A.5.1 Směřování bezpečnosti informací vedením organizace

Cíl: Definovat bezpečnostní politiky, které pokrývají všechny důležité oblasti informační bezpečnosti organizace. Vedení organizace musí vyjádřit podporu a souhlas ve všech činnostech týkajících se uplatňování bezpečností politiky.

A.5.1.1 Politiky pro bezpečnost informací

Opatření: Vytvoření bezpečnostních politik pro bezpečnost informací, které bude vedení organizace plně podporovat. Vedení organizace musí zajistit, aby všichni zaměstnanci byli s politikami řádně seznámeni. Budou rozděleny odpovědnosti a pravomoci spojené s bezpečnostními politikami. Organizace musí nadále projevovat zájem o zlepšování bezpečnosti informací.

Časová náročnost:

- Vytvoření bezpečnostní politiky obce: 30 hodin
- Seznámení zaměstnanců s vytvořenou politikou: 8 hodin

A.5.1.2 Přezkoumání politik pro bezpečnost informací

Opatření: Vedení organizace pověří vlastníka bezpečnostní politiky s odpovědností za tvorbu, přezkoumávání a vyhodnocování politik. Následuje revize politik a přizpůsobení současným potřebám. Přezkoumávání politik bezpečnosti informací v plánovaných časových intervalech. Při změně jakékoli politiky bude nutný souhlas od vedení organizace. Při každé kontrole se zjišťuje, jestli je bezpečnostní politika dobře nastavena a dodržována. Všechny činnosti budou zaznamenávány.

Časová náročnost:

- Vytvoření plánu na přezkoumání bezpečnostních politik: 6 hodin
- Přezkoumání bezpečnostních politik a následné úpravy: 15 hodin/rok

4.3.2 A.6 Organizace bezpečnosti informací

A.6.1 Interní organizace

Cíl: Ustanovit řídící rámec pro zahájení a řízení implementace a provozu bezpečnosti informací v rámci organizace (stanovení rolí a odpovědnosti, atd.).

A.6.1.1 Role a odpovědnosti bezpečnosti informací

Opatření: Všechny odpovědnosti za bezpečnost informací musí být definovány a přiděleny. Přidělování odpovědností musí být v souladu s bezpečnostní politikou organizace. Osoba s přidělenými odpovědnostmi za bezpečnost informací může jednotlivé činnosti delegovat na jiné osoby (odpovědnost však zůstává na ní a měla by rozhodnout, zda byly všechny delegované úkoly provedeny správně). Dále se musí každému aktivu přidělit vlastníka, který za dané aktivum bude zodpovídat. Odpovědná osoba by měla být v dané oblasti kompetentní a měla by dostat možnost udržovat krok s vývojem, aby byla schopná zastávat dané odpovědnosti.

Časová náročnost:

- Rozdělení a definování odpovědností za bezpečnost informací: 20 hodin

A.6.1.2 Princip oddělení povinností

Opatření: Měly by být odděleny konfliktní povinnosti a oblasti působnosti, aby se zmírnily příležitosti pro neoprávněné nebo neúmyslné změny a zneužití aktiv organizace (neměla by nastat situace, kdy bude zaměstnanec povinný vykonávat určitou činnost, odpovědný za jejich výkon sám sobě nebo zaměstnanci na stejném stupni v organizační struktuře organizace). V případech, kdy nelze povinnosti dostatečně oddělit, je důležité alespoň monitorování činností, které jsou s aktivem prováděny. Vytvoření dokumentu s popisem pracovních pozic, kde bude definováno, kdo jaká má práva, role, povinnosti, odpovědnosti s ohledem na vykonávanou činnost pracovní pozice.

Časová náročnost:

- Rozdělení povinností a vytvoření dokumentu s popisem pracovních pozic a jejich povinností: 5 hodin

A.6.1.3 Kontakt s příslušnými orgány a autoritami

Opatření: Toto opatření je již z části aplikováno. Organizace využívá telefonické a emailové spojení s vyššími správními orgány, které zabezpečují možnost konzultací s odborníky. Dále se musí zavést postupy určující, kdy a kým by měly být kontaktovány bezpečnostní autority (např. Národní úřad pro kybernetickou bezpečnost - NÚKIB) a jak mají být identifikované incidenty bezpečnosti informací hlášeny.

Časová náročnost:

- Zavedení postupů nahlašování: 2 hodiny

A.6.1.4 Kontakt se zájmovými skupinami

Toto opatření není nutné zavádět. Jak je zmíněno v **A.6.1.3,** organizace využívá podporu vyšších správních orgánů, které musí zajistit dostatečnou informovanost orgánů nižších.

A.6.1.5 Bezpečnost informací v řízení projektů

Opatření: Začlenit bezpečnost informací do všech částí projektů, aby byla nalezena všechna rizika bezpečnosti informací a díky tomu byla řešena v rámci samotného projektu. Je nutné řešit a pravidelně přezkoumávat dopady bezpečnosti informací ve všech projektech. U používaných metod řízení projektu musí být:

- zahrnuty cíle bezpečnosti informací do projektových cílů,
- prováděno posuzování rizik bezpečnosti informací již v rané fázi projektu, aby se následně identifikovala nezbytná opatření,
- bezpečnost informací součástí všech fází použité projektové metodiky.

Časová náročnost:

- Vytvoření pravidel a návodu na začlenění bezpečnosti informací do všech částí projektů: 5 hodin.

A.6.2 Mobilní zařízení a práce na dálku

Cíl: Zajistit bezpečnost práce na dálku a bezpečnost použití mobilních zařízení.

A.6.2.1 Politika mobilních zařízení

Opatření: Vytvoření a zavedení politiky pro používání mobilních zařízení, aby nemohly být kompromitovány informace týkající se činnosti organizace. Je velmi důležité dávat pozor při používání mobilních zařízení na veřejných místech, v zasedacích místnostech a dalších nechráněných oblastech. Měla by být uplatněna ochrana, která ochrání zařízení před přístupem k informacím nebo prozrazení informací na něm uložených a zpracovávaných (například kryptografická technika), vynucení používání tajných autentizačních informací a softwarová ochrana proti malwaru. Mobilní zařízení by nemělo nikdy zůstat bez dozoru na volně dostupném místě a každý uživatel by si měl dávat pozor při připojování se k veřejným sítím. U každého zařízení musí být nastavena záloha dat, možnost vymazání obsahu nebo zablokování zařízení na dálku v případech krádeže.

Časová náročnost:

- Vytvoření politiky mobilních zařízení: 4 hodiny.

A.6.2.2 Práce na dálku

Opatření: K informacím, ke kterým je přistupováno v rámci práce na dálku, zpracovávaných nebo ukládaných v místech práce na dálku, by měla být vytvořena politika a podpůrná bezpečnostní opatření. Politika by měla definovat podmínky a omezení pro používání práce na dálku. Musí být kladen důraz na zabezpečení komunikace, s přihlédnutím k potřebě vzdáleného přístupu k interním systémům organizace, k citlivosti informací, ke kterým bude přistupováno a které budou přenášeny přes komunikační linky. Důležité je také zavedení ochrany proti malware různých druhů.

Časová náročnost:

- Vytvoření politik pro práci na dálku: 5 hodin

4.3.3 A.7 Bezpečnost lidských zdrojů

A.7.1 Před vznikem pracovního vztahu

Cíl: Zajištění dodržování bezpečnostních politik zaměstnanci a smluvními stranami. Zajištění, aby zaměstnanci a smluvní strany vykonávali úlohy, pro které jsou vhodní.

Budování bezpečnostního povědomí u zaměstnanců, které je svázáno s výkonem funkce dané osoby, aby se lépe minimalizovala bezpečnostní rizika. Zaměstnanci jsou obeznámeni s možností disciplinárního řízení v případě nedodržování politik.

A.7.1.1 Prověřování

Toto opatření je již aplikováno. Uchazeč o zaměstnání v organizaci je prověřen v souladu s platnou legislativou. Při prověřování uchazeče je zohledněn klasifikační stupeň informací, ke kterým bude moci získat přístup, jeho spolehlivost a jsou identifikována potencionální rizika, která sebou uchazeč přináší. Organizace se snaží prověřit si uchazeče u jeho bývalého zaměstnavatele, případně pomocí evidencí rejstříků obsahující informace o dané osobě nebo právním subjektu. U uchazeče si organizace primárně ověřuje: totožnost platným dokladem, profesní životopis, vzdělání a odborné kvalifikace a výpis z trestního rejstříku. Za nábor a prověřování uchazečů odpovídá starosta, popřípadě místostarosta obce.

A.7.1.2 Podmínky pracovního vztahu

Opatření „Podmínky pracovního vztahu“ je aplikováno v pracovní smlouvě. Součástí pracovní smlouvy je samostatný odstavec obsahující závazek mlčenlivosti a určení odpovědnosti za bezpečnost informací pro uchazeče plynoucí z výkonu jeho budoucí pracovní činnosti. Pokud se uzavírají smlouvy s třetími stranami, musí třetí strana podepsat závazek o mlčenlivosti ještě před umožněním přístupu k informacím a prostředkům na zpracování informací v organizaci. Za porušení bezpečnosti informací jsou stanoveny sankce, pokud již nejsou součástí zákoníku práce. Smlouvy jsou uloženy v archivu obecního úřadu.

A.7.2.1 Odpovědnosti vedení organizace

Opatření: Vedoucí zaměstnanci by měli požadovat dodržování bezpečnostních politik od svých podřízených a také od svých smluvních stran. Jsou odpovědní za seznámení podřízených pracovníků s pravidly a povinnostmi, které plynou z bezpečnostních doporučení. Každý zaměstnanec obdrží bezpečnostní pokyny, které jsou vázány na jejich role. Vedení u zaměstnanců zajišťuje udržování příslušných dovedností, potřebnou kvalifikaci a pravidelné vzdělávání.

Časová náročnost:

- Vytvoření politiky odpovědnosti vedení organizace: 6 hodin.

A.7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací

Opatření: Je nutné, aby u zaměstnanců bylo neustále zvyšováno bezpečnostní povědomí formou školení a vzdělávání. Dále musí být zaměstnanci informováni o správném používání prostředků pro přístup a zpracování chráněných informací a o správném dodržování postupu pro zachování bezpečnosti informací. Vzdělávání a školení musí probíhat pravidelně. Organizace by mohla například zavést tyto školení:

1. **Základní školení ISMS**: Toto školení je určeno pro nově nastupující zaměstnance obce (nový zaměstnanec by měl být proškolen ihned po nástupu na svoji pozici, dříve než bude vykonávat jakékoli činnosti týkající se informací organizace).
2. **Školení bezpečnosti informací v pravidelných cyklech**: Zaměstnanci se seznamují s aktuálním stavem bezpečnosti informací, změnami (například legislativními nebo novými technikami řešení bezpečnostních incidentů) a revidují si svoje znalosti v této problematice.
3. **Školení o bezpečnosti informací za mimořádných podmínek:** Probíhá v případech mimořádných změn v zabezpečení informací obce a v případech výskytu významných bezpečnostních incidentů.
4. **Školení pro zaměstnance, kteří budou využívat nové technické vybavení:** Zaměstnanci jsou seznamování s novými postupy při používání systémů a aplikací, které jsou nově zaváděny.
5. **Školení smluvních a třetích stran:** Využívá se v případech, kdy je nutné kvůli povaze činností seznámit smluvní a třetí strany s politikami bezpečnosti informací organizace.

Časová náročnost:

- Vytvoření politiky povědomí, vzdělávání a školení bezpečnosti informací: 5 hodin.
- Školení zaměstnanců: 4 hodiny.

A.7.2.3 Disciplinární řízení

Opatření: V situaci, kdy je ze strany zaměstnance narušena bezpečnost, se vytvoří disciplinární řízení, ve kterém je ověřováno, jestli zaměstnanec pochybil a tím narušil bezpečnost. Disciplinární řízení musí být prováděno tak, aby bylo dodrženo správné a spravedlivé zacházení se zaměstnancem, který je podezřelý z pochybení v tématu bezpečnosti informací (například se zkoumá, jestli byl zaměstnance řádně a včas proškolen). Disciplinární komise nesmí při svém rozhodování a určování trestu porušit platné zákony, a to zejména zákoník práce, občanský zákoník a zákon o úřednících. Podle konečného výroku komise je určen způsob potrestání nebo uhrazení vzniklé škody.

Časová náročnost:

- Vytvoření postupů disciplinárního řízení: 10 hodin.

A.7.3 Ukončení a změna pracovního vztahu

Cíl: Chránit zájmy organizace v rámci změny nebo ukončení pracovního vztahu.

A.7.3.1 Odpovědnosti při ukončení nebo změně pracovního poměru

Toto opatření je již zavedeno. Odpovědnosti a povinnosti nejen v oblasti bezpečnosti informací, které zůstávají v platnosti i po ukončení nebo změně zaměstnání, jsou definovány a sděleny zaměstnanci (i smluvní a třetí straně). Po změně či ukončení pracovní smlouvy musí zaměstnanec dodržovat mlčenlivost, o které byl obeznámen při podepisování smlouvy, na smluvně definované období.

4.3.4 A.8 Řízení aktiv

A.8.1 Odpovědnost za aktiva

Cíl: Identifikace všech aktiv a zajištění jejich přiměřené ochrany vzhledem k charakteru informací.

A.8.1.1 Seznam aktiv

Opatření: Vytvoření seznamu všech identifikovaných aktiv, díky němuž má vedení přehled o všech aktivech v organizaci. Seznam aktiv by měl být aktuální, přesný,

konzistentní a uspořádaný. Příklady aktiv, které mohou být organizací identifikovány, je možné najít v normě ISO/IEC 27005 (identifikace aktiv je důležitý proces při řízení rizik).

Časová náročnost:

- Kontrola a aktualizace seznamu aktiv: 3 hodiny

A.8.1.2 Vlastnictví aktiv

Opatření: Každému identifikovanému aktivu ze seznamu by měl být přidělen vlastník. Vlastníkovi je přidělena odpovědnost za správu a řízení aktiva po dobu životnosti aktiva. Dále by vlastník aktiva měl:

1. provádět inventarizaci aktiv,
2. zajistit náležitou kvalifikaci a ochranu aktiv,
3. stanovit a pravidelně přezkoumávat omezení přístupu k důležitým aktivům a jejich klasifikaci s ohledem na platné politiky řízení přístupu,
4. zajistit správné postupy v případě vymazání či zničení aktiva.

Časová náročnost:

- Přidělení aktiva vlastníkům: 3 hodiny.

A.8.1.3 Přípustné použití aktiv

Opatření: Měla by být identifikována, dokumentována a implementována pravidla pro přípustné používání informací a aktiv spojených s informacemi a vybavením pro zpracování informací. Zaměstnanci a uživatelé z externích stran využívající nebo mající přístup k aktivům organizace, by měli být poučeni o požadavcích bezpečnosti informací na aktiva organizace spojené s informacemi a vybavením pro zpracování informací a zdroji (například citlivé informace by neměly opouštět organizaci, jak prostřednictvím médií nebo sítě správně nezašifrované).

Časová náročnost:

- Vytvoření pravidel pro přípustné použití aktiv: 3 hodiny.

A.8.1.3 Vrácení aktiv

Opatření „Vrácení aktiv“ je již zavedeno. Zaměstnanci a uživatelé z externích stran musí po ukončení svého zaměstnání, smlouvy nebo dohody vrátit všechny aktiva organizace, která měli v držení.

A.8.2 Klasifikace informací

Cíl: Je nutné zajistit, aby informace získala odpovídající úroveň ochrany v souladu s jejím významem pro organizaci.

A.8.2.1 Klasifikace informací

Opatření: Součástí klasifikace informace musí být i určení důležitosti a stupně ochrany pro dané informace. Klasifikována mohou být i jiná aktiva než jenom informace, v souladu s klasifikací informací, která jsou v aktivech uložena, zpracovávána nebo jsou aktivem chráněna. Jednotliví vlastníci aktiv by měli být odpovědní za jejich klasifikaci. Klasifikace poskytuje lidem, kteří se zabývají informacemi, stručnou indikaci, jak s informacemi zacházet a chránit je. Klasifikace by neměla přinášet neúměrné administrativní náklady. U vytváření klasifikace by měla být zohledněna škoda, která nastane v případě zveřejnění nebo prozrazení některých informací. Klasifikační schéma důvěrnosti může vypadat například takto:

1. únik informací nezpůsobí žádné škody,
2. únik informací může způsobit menší provozní obtíže,
3. únik informací má velký krátkodobý dopad na provozní činnosti,
4. únik informací má vážný dopad na dlouhodobé strategické cíle a může ohrozit samotný chod organizace.

Časová náročnost:

- Klasifikace informací: 15 hodin.

A.8.2.2 Označování informací

Opatření: Po klasifikaci všech informací je potřeba, aby byly i správně označeny. Dokumenty jakéhokoli druhu (papírové, elektronické) musejí být označeny vodoznakem nebo hlavičkou s druhem informace (soukromé, citlivé, utajované, veřejné).

Dle označení je pak s informacemi náležitě zacházeno. Zaměstnanci musí být seznámeni se způsobem označení a jak podle označení s informacemi zacházet.
Poznámka: Označování informací a s nimi i souvisejících aktiv může mít i negativní dopad. Klasifikovaná aktiva jsou lépe identifikovatelná, a tím se stávají snadným cílem pro interní krádeže pracovníků nebo externích útočníků. Proto je nutné je mít správně zabezpečené.

Časová náročnost:

- Vytvoření postupu pro označování informací a s nimi souvisejících aktiv: 6 hodin.

A.8.2.3 Manipulace s aktivy

Opatření: Pro zacházení s aktivy by měly být vytvořeny a zavedeny postupy, které budou v souladu se schématem klasifikace informací přijatým organizací. Vytvořit a zavést postupy pro zpracování, ukládání, zacházení a předávání informací v souladu s jejich klasifikací. U každé skupiny informací musíme určit, kdo bude mít oprávnění k využívání informací a vést o tom záznamy. Vytvořené postupy by měly obsahovat:

1. omezení přístupu podporující požadavky na ochranu na každé úrovni klasifikace,
2. tvorbu záznamů o oprávněných příjemcích aktiv,
3. ochrana dočasných nebo trvalých informací musí být shodná s ochranou původních informací,
4. skladování IT aktiv v souladu se specifikacemi výrobce.

Časová náročnost:

- Vytvoření postupů pro manipulaci s aktivy: 4 hodiny.

A.8.3 Manipulace s médii

Cíl: Předcházet neoprávněnému vyzrazení, modifikaci, odstranění nebo zničení informací uložených na médiích.

A.8.3.1 Správa výměnných médií

Opatření: Pro správu médií by měly být zavedeny postupy v souladu se schématem klasifikace přijatých organizací. Pro ukládání důvěrných dat na média je nutné šifrování. Všechna média by měla být evidována a uložená v bezpečném prostředí. Vyřazování médií by mělo probíhat nejlépe fyzickým zničením. Důležitá data by se měla ukládat na více médiích, které budou uloženy na oddělených místech. Je důležité hlídat životnost média a při blížícím se konci nahradit novým médiem, aby nedocházelo ke zbytečné ztrátě dat.

Časová náročnost:

- Vytvoření postupu pro práci a správu výměnných médií: 3 hodiny.

A.8.3.2 Likvidace médií

Opatření: Pokud již média nejsou potřebná nebo jim dochází životnost, měla by být bezpečně zlikvidována dle formálních postupů (média, která mají být zničena a obsahují citlivá data, musí být zničena destruktivním způsobem, a to například skartováním, spálením nebo podobným způsobem, aby se vyloučilo obnovení dat).

Časová náročnost:

- Vytvoření postupů pro likvidaci médií: 2 hodiny.

A.8.3.3 Přeprava fyzických médií

Opatření: Média obsahující informace by měla být během přepravy chráněna před neoprávněným přístupem, zneužitím nebo poškozením (nutnost šifrování informací). Pokud nejsou důvěrné informace na médiích šifrovány, měla by být zvážena dodatečná fyzická ochrana.

Časová náročnost:

- Vytvoření postupů na bezpečnou přepravu fyzických médií: 2 hodiny.

4.3.5 A.9 Řízení přístupu

A.9.1 Požadavky organizace na řízení přístupu

Cíl: Omezit přístup k informacím a k vybavení pro zpracování informací.

A.9.1.1 Politika řízení přístupu

Opatření: Vlastníci aktiv vytvoří přístupová pravidla a oprávnění pro každého dalšího uživatele, který bude používat jejich aktiva. Pravidla musí pokrývat fyzický a logický přístup k zařízení. Dále by se mělo: archivovat záznamy o všech významných událostech, které se týkají používání a správy uživatelských identit a tajných autentizačních informací, pravidelně přezkoumávat přístupové práva, oddělit role v řízení přístupu (např. žádost o přístup, autorizace přístupu, administrace přístupu), brát v úvahu bezpečnostní politiky organizace.

Časová náročnost:

- Vytvoření politik řízení přístupu: 5 hodin.

A.9.1.2 Přístup k sítím a síťovým službám

Opatření: Uživatelům by měl být poskytován pouze přístup k těm sítím a síťovým službám, pro jejichž použití byli výhradně autorizování. Doporučuje se oddělení Wi-Fi sítě od vnitřní sítě a domény (měla by sloužit pouze pro zaměstnance a hosty úřadu pro bezpečný přístup na internet). Neautorizovaná a nezabezpečená připojení k síťovým službám mohou mít vliv na celou organizaci, proto je nutné, aby v politice bylo obsaženo:

1. vytvoření seznamu zaměstnanců, kde bude zaznamenáno, kdo a kam má přístup
2. opatření a postupy pro ochranu a přístup k připojením, k síti a síťovým službám.
3. požadavky na autentizaci pro přístup k síti a síťovým službám
4. monitorování používání síťových služeb.

Časová náročnost:

- Vytvoření politik přístupu k sítím a síťovým službám: 3 hodiny.

A.9.2 Správa a řízení přístupu uživatelů

Cíl: Zajistit oprávněný přístup uživatelů a zabránit neoprávněnému přístupu k systému a službám.

A.9.2.1 Registrace a zrušení registrace uživatele

Toto opatření je aplikováno. Při přidělování přístupových práv je zaveden proces formalizované registrace uživatele včetně jejího zrušení. Za přidělování přístupů k informacím zaměstnanců je odpovědný starosta obce.

A.9.2.2 Správa uživatelských přístupů

Opatření správa uživatelských přístupů je již aplikováno. Pro přidělování a odebírání přístupových práv všem typům uživatelů ke všem systémům a službám je implementován formalizovaný proces správy přístupů.

A.9.2.3 Správa privilegovaných přístupových práv

Opatření: Musí být omezeno a řízeno přidělování a používání privilegovaných přístupových práv. Privilegovaná přístupová práva by měla být přidělována uživatelům na základě potřeby použití a v souladu s politikou řízení přístupu (viz opatření A.9.1.1), to je na základě minimální potřeby pro jejich provozní role. Kompetence uživatelů s privilegovanými přístupovými právy by měly být pravidelně přezkoumávány s cílem ověřit, zda jsou v souladu s jejich pracovními povinnostmi. Je důležité vést záznam o všech přidělených privilegiích.

Časová náročnost:

- Vytvoření politiky správy privilegovaných přístupových práv: 4 hodiny.

A.9.2.4 Správa tajných autentizačních informací uživatelů

Opatření: Přidělení tajných autentizačních informací by mělo být řízeno prostřednictvím formálního procesu řízení. Zaměstnanci by měli být povinni podepsat závazek, že budou udržovat osobní tajné autentizační informace důvěrně a sdílené tajné informace pouze mezi členy organizace (je možné tento závazek dát do pracovní smlouvy).

Časová náročnost:

- Vytvoření politiky na správu tajných autentizačních informací uživatelů: 4 hodiny.

A.9.2.5 Přezkoumání přístupových práv uživatelů

Opatření: Vlastníci aktiv musí přezkoumávat přístupová práva uživatelů v pravidelných intervalech, po každé změně pracovní pozice zaměstnance nebo po ukončení pracovního poměru. Změny týkající se privilegovaných účtů by se měly zaznamenávat formou logu.

Časová náročnost:

- Vytvoření politiky na přezkoumávání přístupových práv uživatelů: 2 hodiny.

A.9.2.6 Odebírání nebo úprava přístupových práv

Toto opatření je již zavedeno. Starosta popřípadě místostarosta je odpovědný za to, aby po ukončení pracovního vztahu zaměstnance byla všechna přístupová práva odebrána popřípadě změněna.

A.9.3 Odpovědnosti uživatelů

Cíl: Učinit uživatele odpovědné za ochranu jejich autentizačních informací.

A.9.3.1 Používání tajných autentizačních informací

Opatření: Po uživatelích by mělo být vyžadováno, aby při používání tajných autentizačních informací dodržovali postupy organizace, z důvodu předcházení neoprávněnému uživatelskému přístupu, prozrazení nebo krádeži informací pomocí správného hesla. Všichni uživatelé by měli být poučeni, aby:

1. udržovali své autentizační informace důvěrné a zajistili, že nejsou vyzrazeny jiným stranám,
2. se vyhnuli jakémukoli záznamu autentizačních informací (papír, soubor, přenosné zařízení, atd.),
3. nahlásili a změnili autentizační informaci kdykoli se vyskytne jakýkoli náznak její možné kompromitace,

4. pokud jsou jako autentizační informace používány hesla, zvolili hesla, která:
    - jsou snadno zapamatovatelná,
    - nejsou založena na osobních informacích,
    - neobsahují po sobě jdoucí abecední nebo číselné znaky,
    - mají minimální délku 8 znaků,
    - obsahují velká a malá písmena, speciální znaky nebo interpunkční znaménko.
5. nepoužívali stejné autentizační informace pro přístup k různým systémům, aplikacím nebo službám,
6. autentizační údaje měnili v pravidelných intervalech (1x za rok).

Časová náročnost:

- Vytvoření politiky pro používání tajných autentizačních informací: 2 hodiny.

A.9.4 Řízení přístupu k systémům a aplikacím

Cíl: Zabránění neoprávněnému přístupu k systému a aplikacím.

A.9.4.1 Omezení přístupu k informacím

Opatření: Přístup k informacím a funkcím aplikačních systémů by měl být omezen v souladu s politikou řízení přístupu. Pro podpoření požadavků na omezení přístupu by se mělo vzít v úvahu:

1. poskytování prostředků pro kontrolu přístupu k funkcím aplikačního systému,
2. pravidelná kontrola dat, ke kterým může konkrétní uživatel přistupovat,
3. kontrolování přístupových práv jiných aplikací,
4. omezování informací obsažených ve výstupech,
5. zajištění fyzického nebo logického řízení přístupu pro izolaci citlivých aplikací, dat nebo systémů.

Časová náročnost:

- Vytvoření politiky na omezení přístupu k informacím: 4 hodiny.

A.9.4.2 Bezpečné postupy přihlášení

Opatření: Postup přihlášení k systému nebo aplikaci by měl být navržen tak, aby se minimalizovala možnost neoprávněného přístupu. Postup přihlášení by proto měl zveřejnit minimum informací o systému nebo aplikaci. Správný postup přihlášení by se měl skládat mimo jiné i z těchto kroků:

1. nezobrazovat identifikátor systému nebo aplikace, dokud nebude proces přihlášení úspěšně dokončen,
2. zobrazovat obecné varovné upozornění, že k počítači by měli přistupovat pouze oprávnění uživatelé,
3. validovat přihlašovací informace pouze po zadání všech vstupních dat. Pokud nastane chybový stav, systém by neměl indikovat, která část je správně nebo nesprávně,
4. neposkytovat pomocné zprávy, které pomohou neoprávněnému uživateli,
5. ochrana před pokusy o přihlášení hrubou silou,
6. logy úspěšných a neúspěšných pokusů,

Časová náročnost:

- Vytvoření politik pro bezpečné postupy přihlášení: 3 hodiny.

A.9.4.3 Systém správy hesel

Opatření: Přihlašování do systému probíhá pomocí ID a hesla. Uživatel si po prvním přihlášení musí změnit heslo podle předchozích politik. Stejné heslo nelze používat vícekrát. Hesla musí být uložena odděleně od aplikačních dat a musí být v šifrované podobě. Hesla se musí povinně pravidelně měnit a nesmí být zobrazována na obrazovce při jejich zadávání.

Časová náročnost:

- Vytvoření politiky správy hesel: 2 hodiny.

A.9.4.4 Použití privilegovaných programových nástrojů

Toto opatření nebude aplikováno. Všechny přístupy k systémům jsou chráněny pomocí přihlašovacích údajů případně jiným podobným bezpečnostním opatřením, proto není potřeba dalších privilegovaných programových nástrojů.

4.3.6 A.10 Kryptografie

A.10.1 Kryptografická opatření

Cíl: Použití kryptografie pro šifrování informací a dat, zajištění jejich autenticity, důvěrnosti a integrity, především u aktiv, u kterých je to nezbytné.

A.10.1.1 Politika pro použití kryptografických opatření

Opatření: Vytvoření politiky, která bude určovat, jak a kdy je nutné použít kryptografické opatření. U každé informace není nutné, stejné úrovně zabezpečení. Pokud informace opouští perimetr organizace, je nutné použít kryptografické opatření (šifrování). Politika by také měla definovat, jak se bude přistupovat ke správě klíčů a metodám obnovení zašifrované informace v případě ztráty, kompromitace nebo poškození klíčů. Pro organizaci typu a velikosti obce, pro kterou jsou tyto politiky vytvářeny, je možné například použít tyto šifrovací programy:

1. **Safetica Personal:** je odlehčená verze edice Bussines. Uživatelské rozhraní má kompletně v češtině a má podobný pás karet jako prostředí Microsoft Office. Poradí si jak s šifrováním virtuálních a fyzických disků, tak i s rychlým zašifrováním konkrétních dat. V oblasti nastavení je velká spousta možností. Jedním z nástrojů navíc je například datová skartovačka, což je nástroj, který vymaže jakoukoli stopu po souboru (soubor už nelze obnovit).
2. **AxCrypt:** jedná se o program šířený pod licencí open source (zdarma). Je to jednoduchý nástroj pro šifrování souborů pomocí algoritmu AES-128. Program se pro pohodlnější používání integruje přímo do kontextového menu Windows Exploreru. Snadno lze nastavit i parametry šifrování a dešifrování, komprese a mazání, prohlížení a editace šifrovaných dat.

3. **VeraCrypt:** je šifrovací nástroj založený na projektu TrueCrypt. Nabízí prakticky totožné funkce. Přesněji jde o vytváření šifrovaných kontejnerů na pevných discích, celých diskových oddílů nebo disků, včetně systémových oddílů. Na rozdíl od svého vzoru poskytuje bezpečnostní vylepšení algoritmů, které zajišťuje imunitu vůči novému vývoji v oblasti útoků hrubou silou, v originálním znění jde o tzv. brute force útoky, což jsou pokusy o rozluštění šifry bez znalosti jejího klíče k dešifrování.

Časová náročnost:

- Vytvoření politiky pro používání kryptografických opatření: 2 hodiny.
- Výběr a aplikace šifrovacího software: 2 hodiny.

A.10.1.2 Správa klíčů

Opatření: Využívání kryptografických opatření vyžaduje správu klíčů. Politika správy klíčů by měla zahrnovat požadavky na správu kryptografických klíčů během jejich celého životního cyklu, včetně generování, ukládání, archivace, znovuzískání, distribuce, vyřazení a zničení klíče. Kryptografické algoritmy, délky klíčů a postupy by měly být v souladu s doporučenými postupy. Musí fungovat mechanismy na dešifrování zašifrovaných dat, pokud dojde k modifikaci či ztrátě klíče.

Časová náročnost:

- Vytvoření politiky správy klíčů: 4 hodiny.

4.3.7 A.11 Fyzická bezpečnost a bezpečnost prostředí

A.11.1 Bezpečné oblasti

Cíl: Předcházet neautorizovanému fyzickému přístupu, poškození a zásahům do informací a vybavení pro zpracování informací organizace. Opatření A.11.1.1 je již zavedeno a stačí k němu přidat rozšíření pro lepší bezpečnost perimetru. Opatření A.11.1.2-4 jsou zavedeny a nepotřebují úpravy či rozšíření. Dále opatření A.11.1.5 a A.11.1.6 není potřeba zavádět z důvodu zaměření organizace.

A.11.1.1 Fyzický bezpečnostní perimetr

Opatření: Měly by být určeny bezpečnostní perimetry a ty by měly být použity k ochraně oblastí, které obsahují buď citlivé nebo kritické informace a vybavení pro zpracování informací. Některá opatření pro fyzický bezpečný perimetr jsou již zavedena, ale mělo by se zvážit jejich rozšíření o tyto pokyny:

1. síla bezpečnostního perimetru by měla záviset na bezpečnostních požadavcích aktiv v rámci perimetru a na výsledcích posuzování rizik,
2. vhodné systémy detekce průniku by měly být nainstalovány dle národních, regionálních nebo mezinárodních norem a pravidelně testovány, aby byly zajištěny všechny vnější dveře a přístupová okna,
3. nevyužité oblasti by měly být neustále zabezpečeny alarmem (nyní jsou chráněny pouze přístupové dveře a hlavní chodba)
4. vybavení pro zpracování informací zpracovávané organizací by mělo být fyzicky odděleno od vybavení spravovaného externími stranami.

Časová náročnost:

- Rozšíření politik pro ochranu fyzického perimetru: 5 hodin.

A.11.2 Zařízení

Cíl: Předejít ztrátě, odcizení, poškození nebo kompromitaci aktiv a díky tomu přerušení provozu organizace.

A.11.2.1 Umístění zařízení a jeho ochrana

Opatření: Zařízení by mělo být umístěno tak, aby byla snížena rizika vyplývající z hrozeb a nebezpečí ze strany životního prostředí a z možnosti neoprávněného přístupu. K ochraně zařízení by se měla zvážit tato opatření:

1. umístění zařízení, aby se minimalizoval zbytečný přístup do pracovních oblastí,
2. zařízení pro práci s citlivými daty by měla být umístěna tak, aby se snížilo riziko sledování informací neoprávněnými osobami,
3. měla by být přijata opatření na snížení rizika potencionálních fyzických nebo environmentálních hrozeb (krádež, požár, kouř, voda, prach, vibrace, atd.)

4. budova by měla být ochráněna před bleskem a všechny přívody energie a komunikační linky by měly být vybaveny filtry na ochranu před bleskem.

Časová náročnost:

- Vytvoření politiky na umístění zařízení a jeho ochrany: 2 hodiny.

A.11.2.2 Podpůrné služby

Opatření: Ochrana zařízení před výpadkem napájení a dalšími poruchami způsobenými selháním podpůrných služeb (elektřina, telekomunikace, atd.). Pro zajištění správné funkčnosti podpůrných služeb je dobré:

1. zajistit pravidelné posuzování a testování vybavení zajišťující podpůrné služby,
2. zajistit včasné upozornění na případnou závadu,
3. implementace redundance (vícenásobné přívody s odlišnými trasami a odlišnými poskytovateli služeb).

Pro předcházení výpadku napájení lze využívat UPS zařízení. Toto zařízení dodává napájení při výpadku elektrické sítě, tak aby se dalo bezpečně ukončit nebo uložit práci a vypnout zařízení dle správných postupů. V každé kanceláři se nachází UPS zařízení, avšak ne každý zaměstnanec ho využívá a u zařízení UPS není pravidelně kontrolována životnost. Je tedy třeba zavést pravidelnou kontrolu a výměnu těchto zařízení a nařídit zaměstnancům jejich používání (dále také připojit všechny síťové prvky na zařízení UPS). Dále by se mělo zřídit redundantní internetové připojení, které se použije při výpadku primárního kabelového připojení (například bezdrátové připojení od mobilních operátorů).

Časová náročnost:

- Aktualizace politiky podpůrné služby: 4 hodiny.

A.11.2.3 Bezpečnost kabelových rozvodů

Opatření: Silová a telekomunikační kabeláž určená pro přenos dat nebo podpůrných informačních služeb by měla být chráněna před odposloucháváním, rušením nebo poškozením. Pro ochranu energetické a komunikační kabeláže by měla být dodržena tato pravidla:

1. je-li to možné, energetická a komunikační rozvodná kabeláž by měla být vedena výhradně ve stěnách a podhledech.
2. žádná kabeláž nesmí být vedena veřejnými prostory odkrytá,
3. energetické a komunikační kabeláže musejí být vedeny odděleně tak, aby se předešlo vzájemnému rušení,
4. zajistit implementaci zvláštních opatření pro citlivé nebo kritické systémy (uzamykatelné skříně, místnosti určené pouze na aktivní prvky, bezpečnostní žlaby, atd.),
5. o rozvodu kabeláže musí být vypracovaná potřebná dokumentace, která musí být pravidelně aktualizována o provedené změny.

Časová náročnost:

- Aktualizace politiky bezpečnost kabelových rozvodů: 12 hodin.

A.11.2.4 Údržba zařízení

Opatření: Z důvodu správné funkčnosti zařízení musí probíhat jeho pravidelná údržba a kontrola. Vedením organizace nebo pověřenou osobou by mělo být zajištěno:

1. opravy budou realizovány pouze odborným pracovníkem nebo firmou, kteří mohou svoji odbornost doložit patřičným dokladem,
2. se zařízeními musí být zacházeno dle pokynů výrobce,
3. zaznamenávání provedených servisních zásahů a kontrol na zařízení,
4. před odesláním zařízení do servisu by měla být zařízení zbavena všech citlivých informací, aby se předešlo úniku citlivých informací,
5. zařízení budou v pravidelných intervalech čištěna od znečištění vnitřních částí prachem, apod. pouze zaškoleným pracovníkem za dohledu zaměstnance obce. Interval čištění nesmí být větší než jeden rok (u některých zařízení i méně).

Časová náročnost:

- Vytvoření plánu a zásad na údržbu zařízení: 4 hodiny.

A.11.2.5 Přemístění aktiv

Opatření: Zařízení, informace nebo software by neměly být přemístěny mimo organizaci bez přechozího povolení vedením organizace. U jakéhokoli přemístění aktiva musí být zdokumentováno, kam bylo přemísťováno, co bylo přemísťováno, kým bylo přemísťováno, na jak dlouho bylo přemísťováno a v jakém stavu bylo navráceno. Je možné zavést namátkové kontroly o vnášení nebo vynášení aktiv.

Časová náročnost:

- Vytvoření politiky pro přemístění aktiv: 2 hodiny.

A.11.2.6 Bezpečnost zařízení a aktiv mimo prostory organizace

Opatření: Používání jakéhokoli zařízení a aktiva pro uchování a zpracování informací mimo organizaci by mělo být schváleno vedením organizace. Toto platí pro zařízení ve vlastnictví organizace a pro zařízení v soukromém vlastnictví používané jménem organizace. Zařízení a média přemístěná mimo prostory organizace by neměla zůstat bez dozoru na veřejných místech a měla by být šifrována. Pokud je zařízení přenášeno mezi různými jednotlivci nebo externími stranami, měl by být veden záznam formou logu, definující řetězec správců zařízení, obsahující minimálně údaje o těch, kteří jsou za zařízení odpovědní. Určitá aktiva obsahující utajované informace by neměla prostory organizace opouštět vůbec.

Časová náročnost:

- Vytvoření politiky pro bezpečnost zařízení a aktiv mimo prostory organizace: 2 hodiny.

A.11.2.7 Bezpečná likvidace nebo opakované použití zařízení

Opatření: U zařízení obsahující paměťová zařízení by mělo být ověřováno, zda neobsahují citlivé informace před opakovaným použitím nebo likvidací. Paměťová zařízení obsahující citlivé informace nebo informace chráněné autorskými právy by měla být fyzicky zničena nebo by měly být obsažené informace zničeny, smazány nebo přepsány díky technikám, které neumožňují obnovení původních informací.

Časová náročnost:

- Vytvoření postupů pro bezpečnou likvidaci nebo opakované použití zařízení: 2 hodiny.

A.11.2.8 Uživatelská zařízení bez obsluhy

Opatření: Uživatelé jednotlivých zařízení by měli zajistit jejich přiměřenou ochranu před neoprávněným použitím v době jejich nevyužívání. Je nutné poučit uživatele o bezpečnostních požadavcích a postupech pro ochranu neobsluhovaných zařízení a o jejich odpovědnosti za tuto ochranu. Uživatelé by měli být informování o tom, aby:

1. ukončili aktivní relace po dokončení činnosti,
2. pokud již nepoužívají aplikace nebo síťové služby, musí se z nich odhlásit,
3. zabezpečovali počítače nebo mobilní zařízení před neoprávněným použitím pomocí zámku nebo rovnocenným opatřením (heslo).
4. po přerušení nebo ukončení činnosti na zařízení, se řádně odhlásili či zařízení zamknuli.

Časová náročnost:

- Vytvoření politiky pro uživatelské zařízení bez obsluhy: 2 hodiny.

A.11.2.9 Zásada prázdného stolu a prázdné obrazovky

Opatření: Pro vybavení, které zpracovává informace, by měla být přijata zásada prázdného stolu, týkající se papírových dokumentů a vyměnitelných paměťových médií a zásada prázdné obrazovky. Zaměstnanci by měli být obeznámeni o důležitosti zachování důvěrnosti informací v elektronické i jiné podobě, ať už na konci pracovního dne nebo i kdykoli během dne, kdy své pracovní místa a stanice opouštějí. V této politice je třeba dosáhnout, aby:

1. kritické nebo citlivé informace organizace v jakékoli podobě byly uzamčeny v době nepoužívání,
2. pracovní stanice byly vždy s odhlášenými uživateli nebo s mechanismem zamykajícím obrazovku, který je opatřen heslem,
3. média obsahující citlivé nebo klasifikované informace by měla být ihned odebrána z tiskáren a podobných zařízení.

Časová náročnost:

- Vytvoření zásady prázdného stolu a prázdné obrazovky: 2 hodiny.

4.3.8 A.12 Bezpečnost provozu

A.12.1 Provozní postupy a odpovědnosti

Cíl: Zajistit správný a bezpečný provoz vybavení pro zpracování informací.

A.12.1.1 Dokumentované provozní postupy

Opatření: Provozní postupy by měly být dokumentovány a být k dispozici všem uživatelům, kteří je potřebují. Měly by být připraveny dokumentované postupy, jako jsou postupy pro zapnutí počítače, konfigurace systému, postupy pro restart a obnovení systému, zálohování, údržbu zařízení, zacházení s médii, správu počítačové místnosti, bezpečnost práce, atd. Dokumentace provozních postupů musí být schválena vedením organizace.

Časová náročnost:

- Vytvoření dokumentace provozních postupů: 4 hodiny.

A.12.1.2 Řízení změn

Opatření: Změny v organizaci, vybavení pro zpracování informací a v systémech, které mají vliv na bezpečnost informací, by měly být řízeny a kontrolovány. Veškeré důležité změny musí být zaznamenány, řízeny a monitorovány. Mělo by se zjistit, jaké budou mít změny dopad na aktiva, uživatele a na bezpečnost informací. Změny by se měly dopředu plánovat a testovat na oddělených částech organizace, aby v případě poruchy neochromily celou organizaci. Všechny příslušné osoby, by měli být seznámeny s podrobnostmi změn.

Časová náročnost:

- Vytvoření politiky řízení změn: 6 hodin.

A.12.1.3 Řízení kapacit

Opatření: Je důležité stále sledovat kapacitní vytíženost zdrojů. Ke každé činnosti, ať už plánované nebo stávající, je třeba identifikovat kapacitní požadavky. Po identifikaci kapacit se musí řídit kapacity zdrojů tak, aby nedocházelo k přetěžování stávajících zdrojů. Mezi kapacitní zdroje patří například počítače, lidské zdroje a další vybavení. Zvláštní pozornost je třeba věnovat zdrojům s dlouhými lhůtami při pořizování nebo vysokými náklady.

Časová náročnost:

- Vytvoření politiky řízení kapacit: 2 hodiny.

A.12.1.4 Princip oddělení prostředí vývoje, testování a provozu

Opatření: Vývojová, testovací a realizovaná úroveň oddělení provozních, testovacích a vývojových prostředí, je nezbytná pro předcházení provozním problémům. U této organizace se jedná hlavně o to, aby testování nebylo prováděno na provozních systémech (viz opatření A.12.1.2) a aby nebylo v testovacích systémech pracováno s citlivými údaji, které nejsou pro testování nezbytné.

Časová náročnost:

- Vytvoření politiky principu oddělení testování a provozu: 4 hodiny.

A.12.2 Ochrana proti malwaru

Cíl: Na ochranu proti malwaru musí být implementována opatření na jeho detekci, prevenci a obnovu, a to ve spojení s odpovídajícím bezpečnostním povědomím uživatelů.

A.12.2.1 Opatření proti malwaru

Toto opatření je již aplikováno. Organizace má postavenou ochranu před malwarem na detekci malwaru, aktualizacích softwaru, na povědomí o bezpečnosti informací a odpovídajících opatření v oblasti přístupu k systému. Organizace pro svoji ochranu používá software ESET NOD 32. Tento software poskytuje komplexní ochranu koncových stanici se systémem Windows, je optimalizován pro virtuální prostředí (dokáže

chránit i útoky na virtuální stroje), umožňuje filtrování přístupu na webové stránky a síťová zařízení, atd.

Časová náročnost:

- Vytvoření opatření proti malwaru: 3 hodiny.

A.12.3 Zálohování

Cíl: Ochrana před ztrátou dat.

A.12.3.1 Zálohování informací

Opatření: Pravidelně by měly být pořizovány a testovány kopie informací, softwaru a bitových kopií systému v souladu se schválenou politikou zálohování. Pro zajištění možnosti obnovy všech důležitých informací a softwaru v případě havárie nebo poruchy médií by měla být zajištěna odpovídající záložní zařízení. Při aktualizaci plánu zálohování se vezmou v úvahu například:

1. měly by být vytvořeny záznamy o záložních kopiích a dokumentované postupy obnovy,
2. rozsah a četnost zálohování by měly odrážet požadavky vyplývající z činností organizace a kritičnosti informací z hlediska kontinuity činností organizace,
3. zálohy by měly být uloženy mimo budovu organizace, aby havárie budovy organizace nezpůsobila škody na zálohovaných informacích,
4. záložním médiím by měla být poskytnuta odpovídající úroveň fyzické ochrany,
5. záložní média by měla být pravidelně testována, aby se předešlo jejich selhání v případě nouzové situace,
6. v případech, kdy záleží na důvěrnosti dat (citlivé informace), by zálohy měly být chráněny pomocí šifrování.

Časová náročnost:

- Aktualizace politiky zálohování informací: 2 hodiny.

A.12.4 Zaznamenávání formou logů a monitorování

Cíl: Zaznamenávat události a vytvářet záznamy.

A.12.4.1 Zaznamenávání událostí formou logů

Opatření: Měly by být pořizovány a pravidelně přezkoumávány záznamy událostí formou logů, které budou zaznamenávat aktivity uživatelů, selhání a události bezpečnosti informací. Dále budou zavedena opatření, která se zaznamenáváním událostí logů úzce souvisí a podporují je.

1. **A.12.4.2 Ochrana logů –** prostředky pro zaznamenávání formou logů a logy musí být chráněny proti zfalšování a neoprávněnému přístupu.
2. **A.12.4.3 Logy a činnosti administrátorů a operátorů –** aktivity systémového administrátora a systémového operátora musí být logovány, tyto logy musí být chráněny a pravidelně přezkoumávány.
3. **A.12.4.4 Synchronizace hodin –** Hodiny všech důležitých systémů pro zpracování informací a logů musí být v rámci organizace nebo bezpečnostních domén synchronizovány s jediným referenčním zdrojem času.

Časová náročnost:

- Vytvoření politiky pro zaznamenávání událostí formou logů: 2 hodiny.
- Vytvoření politiky na ochranu logů: 1 hodina.
- Vytvoření politiky pro logování činnosti administrátorů a operátorů: 1 hodina.
- Vytvoření politiky synchronizace hodin: 1 hodina.
-

A.12.5 Správa provozního software

Cíl: Zajistit integritu provozních systémů.

A.12.5.1 Instalace softwaru na provozní systémy

Opatření: Jakákoli instalace softwaru na provozní systémy musí být předem otestována a musí ji provádět k tomu určená osoba. Instalovaný software musí být předem řádně otestován, aby se předešlo ohrožení provozních systémů v důsledku nesprávné činnosti nebo poruše.

Časová náročnost:

- Vytvoření postupů pro instalaci softwaru na provozní systémy: 2 hodiny.

A.12.6 Řízení technických zranitelností

Cíl: Zabránit využívání technických zranitelností.

A.12.6.1 Řízení technických zranitelností

Opatření: Musí být zajištěno včasné získání informací o existenci technických zranitelností provázaných informačních systémů, vyhodnocena úroveň ohrožení organizace vůči těmto zranitelnostem a přijata opatření na zvládání souvisejících rizik. Měla by se provádět pravidelná kontrola a aktualizace systémů a s tím související evidence využívaných softwarů pro lepší řízení a plánování aktualizací. Aktualizace by se měly instalovat pouze od poskytovatelů softwaru a měly by být testovány pouze na jednom zařízení a po ověření funkčnosti a vyloučení zranitelnosti se mohou instalovat na další zařízení.

Časová náročnost:

- Vytvoření postupů pro řízení technických zranitelností: 3 hodiny.

A.12.6.2 Omezení instalace softwaru

Opatření: Stanovení a implementování pravidel ohledně instalace softwaru uživateli. Toto opatření lze aplikovat například tak, že na uživatelském účtu nebude instalace povolena vůbec a pokud uživatelé budou chtít instalovat jakýkoli software, budou muset požádat pověřenou osobu o povolení a následnou instalaci (pověřená osoba bude mít na pracovní stanici administrátorský účet, přes který bude blokovat instalace popřípadě je provádět).

Časová náročnost:

- Vytvoření postupu pro omezení instalace softwaru: 1 hodina.

4.4 Budování bezpečnostního povědomí

Proces budování bezpečnostního povědomí nikdy nekončí, stejně tak jako je tomu u informační bezpečnosti. Budování bezpečnostního povědomí není závislé na zavedení bezpečnostních opatření a systému řízení informační bezpečnosti, proto by mělo být prováděno zcela nezávisle (i když nejsou zavedeny předchozí systémy). Jedná se o kontinuální proces, kdy rozdělujeme uživatele do skupin a vzděláváme je na několika úrovních podle potřeby organizace. Na proces budování bezpečnostního povědomí se lze dívat třemi způsoby: úrovní vzdělávání (školení, povědomí, vzdělávání, certifikace a profesní rozvoj), funkčního dělení a dělení dle vazeb na ICT, podle skupin uživatelů (začátečník, středně pokročilý, pokročilý). Základním prvkem v budování bezpečnostního povědomí je jeho plán. Plán se skládá z následujících prvků (22):

- Určení rolí a odpovědností – je stanovena odpovědná osoba (manažer kybernetické bezpečnosti). Odpovědnost za budování bezpečnostního povědomí bude mít starosta obce, z důvodu zastupitelnosti bude stanovena druhá osoba a to místostarosta obce, který bude moci také vykonávat budování bezpečnostního povědomí. Starosta bude dohlížet na dodržování plánu, případně jej upravovat a vylepšovat kvůli zajištění co nejvyšší efektivity budování bezpečnostního povědomí.
- Stanovení cílů pro každou úroveň vzdělávání – pro každou úroveň vzdělávání se stanoví cíle, kterých se musí dosáhnout.
- Rozdělení uživatelů do skupin dle znalostí – zaměstnanci budou rozděleni do skupin dle zkušeností a typu využití ICT: běžný uživatel – uživatel, který má pouze základní znalosti o ICT (řadoví zaměstnanci, brigádníci), pokročilý uživatel – uživatel má pokročilejší znalosti o ICT (vedoucí jednotlivých oddělení), specialista – podílí se na zvyšování bezpečnosti informací v organizaci (starosta, místostarosta, pověřená osoba). Příklad srovnávacího rámce bezpečnostního povědomí lze vidět v Tabulce **9**.

Tabulka 9: Srovnávací rámec budování bezpečnostního povědomí. Zdroj: (22)

	Povědomí	Školení	Vzdělání
Vlastnost	„co"	„jak"	„proč"
Úroveň	Informativní	Znalostní	Odborná
Cíl	Rozpoznání a zmapování	Dovednost, zdatnost	Plné porozumění
Cílová skuina	Běžný uživatel, pokročilý uživatel, specialista	Pokročilý uživatel Specialista	Specialista
Vzdělávací metoda	Bezpečnostní kniha, výukové videa, prospekty	Případové studie, praktické ukázky	Diskuze, semináře, studium
Způsob testování vzdělání	Test Ano/ne + otevřené otázky	Řešení problémů (praktická cvičení)	Esej
Časová náročnost	Krátkodobá	Střednědobá	Dlouhodobá

- Ověření vstupních znalostí jednotlivých uživatelů – po ověření jednotlivých uživatelů se rozdělí do skupin, podle kterých je možné blíže specifikovat cíle a rozsah bezpečnostního vzdělávání.
- Určení cílů a vytvoření školících materiálů pro každou skupinu uživatelů.
- Určení problematiky, která se bude v jednotlivých školeních a kurzech řešit.
- Vytvoření metodiky pro nasazení každého aspektu programu.
- Zhotovení dokumentace průběhu výuky a zpětné vazby.
- Vyhodnocení zpětné vazby a aktualizace výukových materiálů.
- Určení četnosti opakování vzdělávání včetně aktualizace výukových materiálů.
- Kalkulace a zhodnocení výsledků vzdělávání.

4.5 GDPR ve vztahu k ISO 27001

Podle GDPR jsou osobní údaje kritické informace, které všechny organizace potřebují chránit. Existují požadavky GDPR, které nejsou v normě ČSN ISO/IEC 27001 zahrnuty. Příkladem je podpora práv subjektů dat (právo být informován, právo být zapomenut nebo právo pro přenositelnost dat). Pokud však organizace zpracovává nebo uchovává osobní údaje, může využít uvedených standardů, které jí pomohou pokrýt velkou část požadavků GDPR.

Hodnocení rizik

Z důvodu vysokých pokut definovaných GDPR a významnému finančnímu dopadu organizace je jasné, že riziko identifikované při hodnocení rizik týkající se osobních údajů je příliš vysoké, aby bylo možné je neřešit. Jedním z požadavků GDPR je posouzení vlivu na ochranu osobních údajů, kde organizace bude muset nejprve analyzovat rizika ochrany osobních údajů stejně jak je požadováno v ČSN ISO/IEC 27001.

Řízení aktiv

Opatření A.8 řízení aktiv z ČSN ISO/IEC 27001 poskytuje podporu činnosti vyžadované Obecným nařízením. Organizace by měly vědět, jaké osobní údaje spravují a zpracovávají, kde jsou uschovány, jak dlouho a kdo k nim má přístup. V těchto požadavcích se plně shoduje s GDPR.

Klasifikace informací

Požadavky na klasifikaci informací jsou obsaženy v normě ČSN ISO/IEC 27001 a definovány opatřením A.8.2.1 (klasifikace informací). ČSN ISO/IEC 27001 uvádí, že informace musí být klasifikovány s ohledem na zákonné požadavky, jejich hodnotu, citlivost a kritičnost proti neoprávněnému prozrazení nebo modifikaci.

Šifrování

ČSN ISO/IEC 27001 doporučuje šifrování jako jedno z opatření, které napomáhá eliminovat rozpoznaná rizika. Otázka implementace kontrol v dané organizaci je prováděna na základě vyhodnocení rizik. Společnosti se systémem podle ISO 27001 mají rizika již identifikována a k nim přiřazena potřebná opatření, takže snadněji dosahují souladu s GDPR

Zvyšování povědomí a odborné přípravy

Pověřenec na ochranu osobních údajů by měl podle GDPR dbát na zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů. Podle opatření A.7.2.2 normy ČSN ISO/IEC 27001 (povědomí, vzdělávání a školení bezpečnosti informací) by měli všichni zaměstnanci organizace a smluvní strany dostávat odpovídající vzdělání a školení pro zvyšování povědomí bezpečnosti informací.

Vývoj, akvizice a údržba systémů

Podle GDPR by ochrana soukromí měla být zohledněna již při vývoji, výběru, koncipování a používání aplikací, služeb a produktů. Opatření A.14 (akvizice, vývoj a údržba systémů) zajišťuje, aby se bezpečnost informací stala nedílnou součástí informačních systémů v jejich životním cyklu.

Dodavatelské vztahy

Podle GDPR mohou být vztahy správců a zpracovatelů založeny na standartních doložkách o ochraně údajů přijaté Komisí nebo Úřadem na ochranu osobních údajů, které mohou být začleněny do rozsáhlejších smluv s širšími smluvními závazky. Opatření A15.1 normy ČSN ISO/IEC 27001 (bezpečnost informací v dodavatelských vztazích) se zaměřuje na ochranu aktiv organizace, ke kterým mají dodavatelé přístup.

Oznamování bezpečnostních incidentů

Podle GDPR budou muset organizace do 72 hodin po zjištění oznámit narušení bezpečnosti osobních údajů Úřadu pro ochranu osobních údajů. Opatření A16.1 ČSN ISO/IEC 27001 (řízení incidentů bezpečnosti informací a zlepšování) vyžaduje odpovídající a efektivní přístup ke zvládání bezpečnosti informací zahrnující komunikaci ohledně bezpečnostních událostí a slabých míst. Tento systém řízení incidentů formalizovaný podle ČSN ISO/IEC 27001 významně pomůže při plnění povinností nařízení GDPR.

Shoda a předpisy

Při implementaci normy ČSN ISO/IEC 27001 je kvůli opatření A.18.1.1 (identifikace odpovídající legislativy a smluvních požadavků) vytvořena povinnost mít k dispozici seznam příslušných legislativních, předpisových a smluvních požadavků. Proto GDPR musí být součástí takového seznamu. Dále v opatření A.18.1.4 (soukromí a ochrana osobních údajů) je vyžadována ochrana osobních údajů v souladu s odpovídající legislativou a předpisy.

Norma ISO 27001 stanovuje požadavky na ustanovení, implementování, udržování a neustálé zlepšování informační bezpečnosti v rámci kontextu organizace. Zakládá si na strukturované dokumentaci a na organizačních a technických opatřeních. Zaměstnanci organizací se zavedenými systémy řízení informací a kybernetické bezpečnosti

(ČSN ISO/IEC 27001) jsou si vědomi svých povinností vůči informacím a jsou proškoleni pro práci s citlivými informacemi. Norma ČSN ISO/IEC 27001 je dobrým základem pro rychle dosažitelný a udržitelný soulad s GDPR.

K souladu s požadavky Obecného nařízení o ochraně osobních údajů napomáhají například následující opatření, která jsou zavedena v první etapě:

- A.6.1.1 Role a odpovědnosti bezpečnosti informací,
- A.6.1.3 Kontakt s příslušnými orgány a autoritami,
- A.7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací,
- A.8.2.1 Klasifikace informací,
- A.9.2.5 Přezkoumání přístupových práv uživatelů,
- A.9.4.1 Omezení přístupu k informacím,
- A.12.4.1 Zaznamenávání událostí formou logů.

4.6 Přezkoumání, údržba, monitorování, a zlepšování ISMS

Zajištění bezpečnosti informací je nikdy nekončící proces, který je nutné neustále kontrolovat a zlepšovat. Při vytvoření bezpečnostní politiky v obci a při vyjádření podpory vedení obce k řešení bezpečnosti informací se nastartoval koloběh soustavného procesu ISMS. Tento proces není nikdy ukončen a musí stále docházet k jeho zlepšování tak, jak k tomu navádí Demingův model PDCA. Na zavedená opatření vybraná z normy ČSN ISO/IEC 27001 je u každého z nich stanoven plán pravidelných kontrol a monitorování bezpečnostních incidentů. Je důležité, aby odpovědní pracovníci byli dostatečně seznámeni s důležitostí bezpečnosti informací a snažili se neustále vyhledávat nové hrozby, ze kterých by mohly vzniknout rizika. Oblast ICT má velice rychlý růst. S tímto rychlým růstem však přichází i růst hrozeb, které mohou na ICT působit. Proto je důležité využívat při ochraně před těmito hrozbami proaktivní přístup (zaměstnanci, kteří zodpovídají za bezpečnost, se musí neustále vzdělávat v novinkách, týkající se bezpečnosti, a tím budou zlepšovat systém ISMS celé organizace).

4.7 Postup zavedení první etapy

Cílem první etapy je zavést opatření pro eliminaci hrozeb s vysokou mírou rizika a zavést opatření, která pomohou při plnění souladu s Obecným nařízením o ochraně osobních údajů.

S nejvyšší mírou rizika na obec působí hrozba špatného zabezpečení budovy, výpadek elektřiny, poškození požárem, napadení virem a porušení mlčenlivosti. Z toho důvodu je dle mého názoru dobré nejprve zavést opatření, která jsou označena jako A.11 Fyzická bezpečnost a bezpečnost prostředí. Těmito opatřeními lze předejít ztrátám, poškozením a případnému zneužití aktiv. Další na řadě budou opatření ze skupiny A.10 Kryptografie, která pokryjí vypracování politik pro šifrování aktiv. Díky této skupině opatření by měla být zabezpečena aktiva proti neoprávněnému použití a při jejich ztrátě. Dalšími opatřeními budou A.9 Řízení přístupu a A.8 Řízení aktiv. Tyto opatření zajišťují a identifikují přiměřenou ochranu aktiv a klasifikují informace dle důležitosti. Dále budou následovat opatření ze skupin A.5 Politika bezpečnosti informací a A.6 Organizace bezpečnosti informací. Při aplikaci těchto politik jsou definovány role a odpovědnosti pro nakládání s informacemi a je zajištěno pravidelné přezkoumávání a doplňování politik pro bezpečnost informací. Tyto politiky spolu blízce souvisí a je dobré je zavádět po sobě. Následuje skupina opatření A.7 Bezpečnost lidských zdrojů, jejíchž obsahem je vybudování kvalitního bezpečnostního povědomí mezi zaměstnanci organizace. Zaměstnanci a uživatelé si musí být vědomi nutnosti dodržování bezpečnostních pravidel a musí se podle nich řídit. Bezpečnostní povědomí v organizaci je považováno za klíčový prvek v systému řízení bezpečnosti informací. Poslední skupinou opatření, která bude v první etapě zaváděna je A.12 Bezpečnost provozu. Tímto opatřením bude zajištěn správný a bezpečný provoz vybavení pro zpracování informací a bude neustále snižována možnost narušení bezpečnosti provozu z důvodu instalace škodlivých softwarů.

4.7.1 Ekonomické zhodnocení a časový harmonogram

Organizace se rozhodla zavádět opatření ve dvou etapách z toho důvodu, že si nemůže kvůli nedostatečnému rozpočtu dovolit uvolnit nebo najmout zaměstnance, který by se plně věnoval zavádění ISMS. Ze stejného důvodu organizace nemůže vyhradit zaměstnance na Obecné nařízení o ochraně osobních údajů, proto bude najata externí firma, která se by se měla o vše v tomto ohledu postarat. Jak již bylo zmíněno výše, opatření

z normy ČSN ISO/IEC 27001 mohou velice pomoci při přípravě na Obecné nařízení o ochraně osobních údajů. Nařízení vstoupí v platnost 25.května letošního roku, proto je nutné, aby se zvládly obě etapy zavést ještě před tím, než bude najata externí firma. O termínu a způsobu zavádění druhé etapy bude rozhodnuto na základě časových možností organizace až po úspěšném zavedení opatření z první etapy. Časovou náročnost a náklady první etapy, lze vidět v Tabulce **10**.

Tabulka 10: Časová náročnost a náklady první etapy. Zdroj: vlastní zpracování

Opatření	Časová náročnost[h]		Náklady [odhad Kč]	
	Zavedení	Ročně	Zavedení	Ročně
A.5.1.1	38	4	15 200,00 Kč	1 600,00 Kč
A.5.1.2	6	15	2 400,00 Kč	6 000,00 Kč
A.5	44	19	17 600,00 Kč	7 600,00 Kč
A.6.1.1	20	1	8 000,00 Kč	400,00 Kč
A.6.1.2	5	1	2 000,00 Kč	400,00 Kč
A.6.1.3	2	1	800,00 Kč	400,00 Kč
A.6.1.5	5	1	2 000,00 Kč	400,00 Kč
A.6.2.1	4	1	1 600,00 Kč	400,00 Kč
A.6.2.2	5	1	2 000,00 Kč	400,00 Kč
A.6	41	6	16 400,00 Kč	2 400,00 Kč
A.7.1.1	0	1	0,00 Kč	400,00 Kč
A.7.1.2	0	1	0,00 Kč	400,00 Kč
A.7.2.1	6	1	2 400,00 Kč	400,00 Kč
A.7.2.2	9	4	3 600,00 Kč	1 600,00 Kč
A.7.2.3	10	1	4 000,00 Kč	400,00 Kč
A.7.3.1	0	1	0,00 Kč	400,00 Kč
A.7	25	9	10 000,00 Kč	3 600,00 Kč
A.8.1.1	3	1	1 200,00 Kč	400,00 Kč
A.8.1.2	3	1	1 200,00 Kč	400,00 Kč
A.8.1.3	3	1	1 200,00 Kč	400,00 Kč
A.8.1.4	0	1	0,00 Kč	400,00 Kč
A.8.2.1	15	5	6 000,00 Kč	2 000,00 Kč
A.8.2.2	6	2	2 400,00 Kč	800,00 Kč
A.8.2.3	4	1	1 600,00 Kč	400,00 Kč
A.8.3.1	3	1	1 200,00 Kč	400,00 Kč
A.8.3.2	2	1	800,00 Kč	400,00 Kč
A.8.3.3	2	1	800,00 Kč	400,00 Kč
A.8	41	15	16 400,00 Kč	6 000,00 Kč
A.9.1.1	5	1	2 000,00 Kč	400,00 Kč
A.9.1.2	3	1	1 200,00 Kč	400,00 Kč
A.9.2.1	0	1	0,00 Kč	400,00 Kč

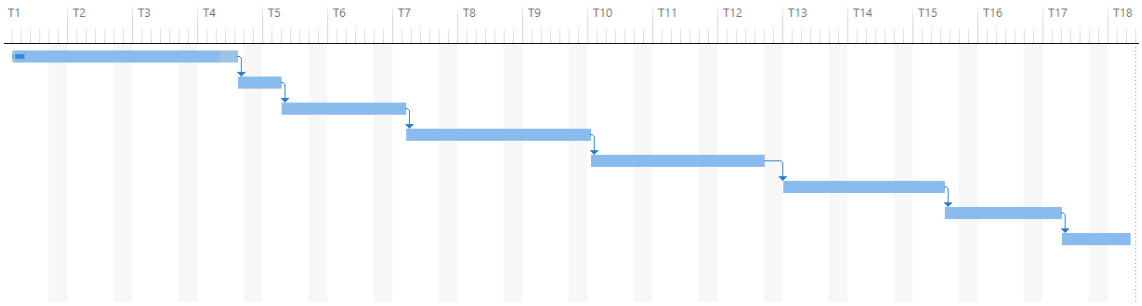
A.9.2.2	0	1	0,00 Kč	400,00 Kč
A.9.2.3	4	1	1 600,00 Kč	400,00 Kč
A.9.2.4	4	1	1 600,00 Kč	400,00 Kč
A.9.2.5	2	1	800,00 Kč	400,00 Kč
A.9.2.6	0	1	0,00 Kč	400,00 Kč
A.9.3.1	2	1	800,00 Kč	400,00 Kč
A.9.4.1	4	1	1 600,00 Kč	400,00 Kč
A.9.4.2	3	1	1 200,00 Kč	400,00 Kč
A.9.4.3	2	1	800,00 Kč	400,00 Kč
A.9	29	12	11 600,00 Kč	4 800,00 Kč
A.10.1.1	4	1	1 600,00 Kč	400,00 Kč
A.10.1.2	4	1	1 600,00 Kč	400,00 Kč
A.10	8	2	3 200,00 Kč	800,00 Kč
A.11.1.1	5	1	7 000,00 Kč	400,00 Kč
A.11.1.2	2	1	800,00 Kč	400,00 Kč
A.11.1.3	4	1	1 600,00 Kč	400,00 Kč
A.11.1.4	12	1	4 800,00 Kč	400,00 Kč
A.11.2.1	4	2	19 600,00 Kč	800,00 Kč
A.11.2.2	2	1	8 800,00 Kč	400,00 Kč
A.11.2.3	12	1	4 800,00 Kč	400,00 Kč
A.11.2.4	4	1	1 600,00 Kč	400,00 Kč
A.11.2.5	2	1	800,00 Kč	400,00 Kč
A.11.2.6	2	1	800,00 Kč	400,00 Kč
A.11.2.7	2	2	800,00 Kč	800,00 Kč
A.11.2.8	2	1	800,00 Kč	400,00 Kč
A.11.2.9	2	1	800,00 Kč	400,00 Kč
A.11	55	15	53 000,00 Kč	6 000,00 Kč
A.12.1.1	4	1	1 600,00 Kč	400,00 Kč
A.12.1.2	6	1	2 400,00 Kč	400,00 Kč
A.12.1.3	2	1	800,00 Kč	400,00 Kč
A.12.2.1	3	1	1 200,00 Kč	400,00 Kč
A.12.3.1	2	1	800,00 Kč	400,00 Kč
A.12.4.1	2	1	800,00 Kč	400,00 Kč
A.12.4.2	1	1	400,00 Kč	400,00 Kč
A.12.4.3	1	1	400,00 Kč	400,00 Kč
A.12.4.4	1	1	400,00 Kč	400,00 Kč
A.12.5.1	2	1	800,00 Kč	400,00 Kč
A.12.6.1	3	1	1 200,00 Kč	400,00 Kč
A.12.6.2	1	1	400,00 Kč	400,00 Kč
A.12	28	12	11 200,00 Kč	4 800,00 Kč
Celkem	271	90	139 400,00 Kč	36 000,00 Kč

Poslední řádek tabulky ukazuje celkový odhad nákladů na první etapu. Připravení úvodní dokumentace a počáteční zavedení a nastavení potrvají odhadem 271 hodin. Činnosti, které se opakují ročně, budou trvat 90 hodin (po prvním roce se bude počet hodin snižovat). Hodinovou mzdu pro bezpečnostního specialisty, který bude interním zaměstnancem organizace, odhaduji na 400 Kč/h (na zavádění ISMS má vymezeno 15 hodin týdně). Pokud by se organizace rozhodla využít externího specialisty, byla by výše mzdy minimálně 1000 Kč/h.

Po sečtení času všech skupin opatření z první etapy byl sestaven časový harmonogram, který lze vidět na Obrázku **11** a Obrázku **12**.

Název úkolu	Doba trvání	Zahájení	Dokončení	Předchůdci
A.11 Fyzická bezpečnost a bezpečnost prostředí	55 hodin	04.09. 17	29.09. 17	
A.10 Kryptografie	8 hodin	29.09. 17	03.10. 17	1
A.9 Řízení přístupu	29 hodin	04.10. 17	17.10. 17	2
A.8 Řízení aktiv	41 hodin	17.10. 17	06.11. 17	3
A.5 Politika bezpečnosti informací	44 hodin	06.11. 17	24.11. 17	4
A.6 Organizace bezpečnosti informací	41 hodin	27.11. 17	14.12. 17	5
A.7 Bezpečnost lidských zdrojů	25 hodin	14.12. 17	26.12. 17	6
A.12 Bezpečnost provozu	17 hodin	27.12. 17	03.01. 18	7

Obrázek 11: Časový harmonogram. Zdroj: vlastní zpracování



Obrázek 12: Časová osa. Zdroj: vlastní zpracování

Odhad celkových nákladů na první etapu včetně návrhu na zavedení bezpečnostních opatření je 139 400 Kč. Tento odhad je pouze orientační a může se měnit v závislosti na časové náročnosti prováděné dokumentace, průběhu zavádění, ceně jednotlivých komponentů a jejich nastavení. Každý rok je nutné započítat roční náklady 41 000 Kč, které slouží na revizi, audit a udržování opatření. Obec na zavedení první etapy odsouhlasila rozpočet 200 000 Kč z důvodu rezerv pro jednotlivé zavádění opatření. Propočet těchto hodnot lze vidět v Tabulce **11**.

Tabulka 11: Ekonomické zhodnocení: Zdroj: vlastní zpracování

	Jednorázová časová náročnost	Roční časová náročnost	Jednorázové náklady	Roční náklady
Návrh bezpečnostních opatření	**122**	**0**	**48 800,00 Kč**	**0**
Zavedení bezpečnostních opatření	**149**	**0**	**90 600,00 Kč**	**0**
Audit zavedených opatření	**0**	**90**	**41 000,00 Kč**	**41 000,00 Kč**
Celkem	**271**	**90**	**139 400,00 Kč**	**41 000,00 Kč**

Druhá etapa zavádění opatření je plánovaná tak, aby se stihla ukončit před najmutím externí firmy na Obecné nařízení o ochraně osobních údajů.

4.8 Přínos práce

Za hlavní přínosy této práce považuji zvýšení bezpečnosti informací ve vybrané obci a lepší připravenost na Obecné nařízení o ochraně osobních údajů. Vedení si díky provedené analýze uvědomilo možná rizika a jejich dopady při neadekvátním zabezpečení organizace. Pokud by se v budoucnu zavedlo ISMS v celém rozsahu, bylo by možné usilovat o certifikaci. Certifikace může vést k rozšíření působnosti a pravomocí obce (což povede k většímu rozpočtu uděleným státem). Jak již bylo v práci zmíněno, řízení bezpečnosti informací je nikdy nekončící proces. Pokud tak organizace bude činit, měla by se úroveň bezpečnosti neustále zvyšovat a zlepšovat.

Tato práce může být základní metodikou postupu při zavádění systému řízení bezpečnosti informací v menší obci. Ke zvýšení informační bezpečnosti nedochází pouze navržením opatření, na výsledek analýzy rizik, ale také zavedením bezpečnostních opatření spadajících do oblasti interní bezpečnosti informací, jejichž zavedení bylo navrženo z důvodu jejich obecné působnosti v oblasti bezpečnosti informací a také z důvodu přípravy na Obecné nařízení na ochranu osobních údajů. Obecné nařízení o ochraně osobních údajů, které nabývá účinnosti dne 25. května letošního roku, je trnem v oku mnoha společnostem a organizacím, takže i z tohoto důvodu byla vytvořena tato doporučení dle normy ČSN ISO/IEC 27001, které jsou při přípravě na nařízení velice nápomocná (v práci je sepsán soulad opatření normy ČSN ISO/IEC 27001 s požadavky Obecného nařízení na ochranu osobních údajů v Kapitole 3). Organizace počítá s tím, že v době nabytí účinnosti nařízení bude první etapa zavádění opatření již ukončena a druhá etapa bude ukončená nebo téměř před ukončením. Pokud by se roz-

hodla obec pro zpracování projektu komerční cestou v podobném rozsahu, jako obsahuje tato práce, musela byt investovat desítky tisíc korun. Což by hodně ovlivnilo výsledný rozpočet.

Dle mého názoru je pro obec největším přínosem pochopení hrozby nezájmu v oblasti bezpečnosti informací. Vedení obce si uvědomilo, že v dnešní době je nutné zabudovávat prvky bezpečnosti téměř do všech činností, které provádí. Dále jsem vypracoval seznam opatření druhé fáze podle normy ČSN ISO/IEC 27001 a prohlášení o aplikovatelnosti, které se nacházejí v Příloze **1** a Příloze **2.**

ZÁVĚR

Cílem této diplomové práce bylo navržení souboru doporučení pro eliminaci nebo redukci zjištěných hrozeb dle ISMS s využitím řady norem ISO/IEC 27000 a využitím tohoto souboru doporučení při samotné přípravě na Obecné nařízení o ochraně osobních údajů. Práce byla zpracovávána pro menší obec, která v současnosti nemá komplexně zpracované a řádně zdokumentované procesy bezpečnosti informací. Z důvodu platných zákonů, kterým organizace podléhá a nově platného nařízení EU o ochraně osobních údajů, by mělo vedení organizace zvážit dlouhodobou udržitelnost současného stavu. Obec se rozhodla, že prozatím nebude usilovat o certifikaci. Proto bylo zavádění opatření rozděleno do dvou etap tak, aby byl proces zavádění co nejkvalitnější, bez zbytečných chyb a v souladu s možnostmi obce.

Z provedené analýzy rizik bylo zjištěno, že obec trpí velkými nedostatky z pohledu bezpečnosti informací a zařízení pro zpracování informací a bezpečnostními mezerami téměř ve všech oblastech své činnosti, což by způsobovalo velké problémy při dosahování souladu s Obecným nařízením o ochraně osobních údajů. Na základě teoretických znalostí norem pro řízení bezpečnosti informací a možnostech vedení obce jsem navrhnul, dle mého názoru co nejlepší variantu pro řešení zavádění opatření dle ISMS. Všechny záležitosti, které se týkaly návrhu a zavádění opatření dle ISMS jsem konzultoval se starostou obce tak, aby výsledné řešení bylo reálně použitelné. Díky provedené analýze rizik (identifikace aktiv, ohodnocení aktiv, identifikace hrozeb, atd.) byla navržena opatření, která jednotlivá rizika eliminují na přijatelnou úroveň. Jedním z podstatných aspektů správného fungování ISMS je kvalitní budování bezpečnostního povědomí, na které jsem sepsal návod pro jeho správné vykonávání.

Podle mého názoru se mi povedlo splnit cíle práce, a to úspěšně vytvořit soubor doporučení pro eliminaci nebo redukci zjištěných hrozeb dle ISMS, s využitím řady norem ISO/IEC 27000 a využitím tohoto souboru doporučení při samotné přípravě na Obecné nařízení o ochraně osobních údajů. Tato práce pomohla obci, aby si uvědomila rizika spojená se špatným nakládáním s informacemi a nesystematickým řešením samotné bezpečnosti informací. Za předpokladu, že se bude obec i nadále věnovat správnému rozvoji ISMS a zavedení druhé etapy opatření, bude možné uvažovat o certifikaci, což by mohlo vést k rozšíření působnosti a zvýšení správních pravomocí.

Obec práci převzala a na jejím základě zvažuje další postupy směřující k zavedení opatření dle ISMS v obci.

BIBLIOGRAFIE

(1) POŽÁR, Josef. *Manažerská informatika*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN ISBN978-80-7380-276-9.

(2) ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Vyd. 1. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

(3) BÉBR, Richard a Petr DOUCEK. *Informační systémy pro podporu manažerské práce*. 1. vyd. Praha: Professional Publishing, 2005. ISBN 978-808-6419-794.

(4) DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

(5) JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

(6) *ČSN ISO/IEC 27000: Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnostní informací – Přehled a slovník*. Praha: Úřad pro technickou normalizaci, 2014.

(7) All about ISO. *Iso.org* [online]. b.r. [cit. 2018-05-05]. Dostupné z: https://www.iso.org/about-us.html

(8) All about the IEC. *Iec.ch* [online]. b.r. [cit. 2018-05-05]. Dostupné z: http://www.iec.ch/about/?ref=menu

(9) Mezinárodní telekomunikační unie: ITU. *Mpo.cz* [online]. b.r. [cit. 2018-05-05]. Dostupné z: https://www.mpo.cz/cz/e-komunikace-a-posta/elektronicke-komunikace/mezinarodni-vztahy/mezinarodni-telekomunikacni-unie--itu--70145/

(10) O úřadu. *Unmz.cz* [online]. b.r. [cit. 2018-05-05]. Dostupné z: http://www.unmz.cz/urad/o-uradu

(11) *ČSN ISO/IEC 27001: Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky*. Praha: Český normalizační institut, 2014.

(12) *ČSN ISO/IEC 27002: Informační technologie - Bezpečnostní techniky – Systémy*

řízení bezpečnosti informací - Požadavky. Praha: Úřad pro technickou normalizaci, 2014.

(13) *ČSN ISO/IEC 27003: Informační technologie - Bezpečnostní techniky - Směrnice pro implementaci systému řízení bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, 2012.

(14) *ČSN ISO/IEC 27004: Informační technologie - Bezpečnostní techniky - Řízení bezpečnosti informací - Měření*. Praha: Úřad pro technickou normalizaci, 2011.

(15) *ČSN ISO/IEC 27005: Informační technologie - Bezpečnostní techniky – Řízení rizik bezpečnosti informací - Přehled a slovník*. Praha: Český normalizační institut, 2014.

(16) Jak volit nástroje pro snižování rizika. *QMprofi.cz* [online]. b.r. [cit. 2018-05-05]. Dostupné z: https://www.qmprofi.cz/33/jak-volit-nastroje-pro-snizovani-rizika-uniqueidgOkE4NvrWuOKaQDKuox_ZzO5vQWd302LM1psNPebI4g/

(17) E-ISO: ISO 27001. *EISO.cz* [online]. b.r. [cit. 2018-05-05]. Dostupné z: http://www.eiso.cz/poradenstvi/zavadeni-systemu/ISO-27001/

(18) ITIL 2011. *Bestpractice.cz* [online]. b.r. [cit. 2018-05-05]. Dostupné z: https://www.bestpractice.cz/Files/Documents/itil_2011_summary_of_updates.pdf

(19) Procesní řízení IT. *Dcit.cz* [online]. b.r. [cit. 2018-05-05]. Dostupné z: https://www.dcit.cz/cs/konzultace/procesni-rizeni-IT

(20) *Ochrana osobních údajů: zákon o ochraně osobních údajů a další právní předpisy. GDPR - obecné nařízení Evropského parlamentu a rady (EU) 2016/679, o ochraně osobních údajů : redakční uzávěrka 28.8.2017*. Ostrava: Sagit, 2017. ÚZ. ISBN 978-80-7488-241-8.

(21) 2. Nové přístupy a povinnosti. *Uoou.cz* [online]. b.r. [cit. 2018-05-05]. Dostupné z: https://www.uoou.cz/2-nove-p-istupy-a-povinnosti/d-27268

(22) Building an Information Technology Security Awareness and Training Program. *Citadel-information.com* [online]. b.r. [cit. 2018-05-05]. Dostupné z: http://citadel-information.com/wp-content/uploads/2012/08/nist-sp800-50-building-information-security-awareness-program-2003.pdf

SEZNAM ZKRATEK

ČSN - Česká technická norma

ICT - Informační a komunikační technologie

IS - Informační systém

ISO - Mezinárodní organizace pro normalizaci

ISMS - Systém řízení bezpečnosti informací

IT - Informační technologie

LAN - Lokální síť

PDCA - Demingův cyklus (Plánuj, dělej, kontroluj, jednej)

IEC - Mezinárodní úřad pro elektrotechniku

UPS - Nepřerušitelný zdroj napájení

Wi-Fi - Bezdrátová síť

COBIT - Standard pro správné postupy řízení informačních technologií

ITIL - Knihovna infrastruktury informačních technologií

EU – Evropská unie

DPIA - Posuzování vlivu na ochranu osobních údajů

SEZNAM TABULEK

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

PŘÍLOHA Č. 1: Seznam opatření druhé etapy podle ČSN ISO/IEC 27001

Tabulka 12 :Seznam opatření druhé etapy. Zdroj: vlastní zpracování

Označení	Opatření	Popis opatření
A.13	**Bezpečnost komunikací**	
A.13.1	Správa bezpečnosti sítě	
A.13.1.1	Opatření v sítích	Síťový provoz musí být řízen a kontrolován v zájmu zachování bezpečnosti. Je nutné přijmout opatření, která zajistí bezpečnost přenášených dat a nemožnost jejich změny.
A.13.1.2	Bezpečnost síťových služeb	Dohody o poskytování síťových služeb musí obsahovat bezpečnostní mechanismy, úroveň poskytovaných služeb a požadavky na správu všech síťových služeb.
A.13.1.3	Princip oddělení v sítích	V síti musí být odděleny skupiny informačních služeb, uživatelů a informačních systémů.
A.13.2	Přenos informací	
A.13.2.1	Politiky a postupy při přenosu informací	Pro interní i externí přenos informací se musí zavést politiky, aby se informace zajistily proti nevyžádané změně, odposlechnutí nebo neoprávněnému použití.
A.13.2.2	Dohody o přenosu informací	Dohody se musí zabývat zabezpečeným přenosem informací týkající se činností organizace mezi organizací a externími stranami.
A.13.2.3	Elektronické předávání zpráv	Elektronické zprávy musí být přiměřeně chráněny (například použitím elektronického podpisu). Pro předávání zpráv je zakázáno použít jiných komunikačních kanálu než přes povolenou emailovou schránku.
A.14	**Akvizice, vývoj a údržba systémů**	
A.14.1	Bezpečnostní požadavky informačních systémů	
A.14.1.1	Analýza a specifikace požadavků bezpečnost informací	V požadavcích na nové informační systémy nebo rozšíření existujících systémů musí být také obsaženy požadavky týkajících se bezpečnosti informací.
A.14.1.2	Zabezpečení aplikačních služeb ve veřejných sítích	Informace obsažené v aplikačních vrstvách využívané pro veřejnou komunikaci musí být chráněny.

A.14.1.3	Ochrana transakcí aplikačních služeb	Informace transakcí aplikačních služeb musí být chráněny, aby se předešlo neoprávněné změně nebo chybnému přenosu.
A.14.2	Bezpečnost v procesech vývoje a podpory	
A.14.2.3	Technické přezkoumání aplikací po změnách provozní platformy	V případě změny provozní platformy musí být otestovány a přezkoumány aplikace kritické pro činnosti organizace, aby se zajistilo, že změny nemají nepříznivý dopad na provoz nebo bezpečnost organizace.
A.14.2.5	Principy budování bezpečných systémů	Principy budování bezpečnostních systémů musí být ustanoveny, dokumentovány, udržovány a aplikovány při implementaci informačních systémů.
A.14.2.9	Testování akceptace systémů	Při aktualizaci informačního systému na novější verzi musí proběhnout testování informačního systému na správnou funkčnost a bezpečnost.
A.15	**Dodavatelské vztahy**	
A.15.1	Bezpečnost informací v dodavatelských vztazích	
A.15.1.1	Politika bezpečnosti informaci pro dodavatelské vztahy	Požadavky bezpečnosti informací na snížení rizik spojených s přístupem dodavatelů k aktivům organizace musí být odsouhlaseny s dodavateli a dokumentovány.
A.15.1.2	Bezpečnostní požadavky v dohodách s dodavateli	Za předpokladu, že dodavatel získává přístup k informacím společnosti (přenos, ukládání, správa), musí se smluvně zajistit požadavky na bezpečnost informací.
A.15.1.3	Dodavatelský řetězec informačních a komunikačních technologií	Dohody s dodavateli musí zahrnovat požadavky na rizika bezpečnosti informací spojená s dodavatelským řetězcem služeb a produktů informačních a komunikačních technologií.
A.15.2	Řízení dodávek služeb dodavatelů	
A.15.2.1	Monitorování a přezkoumávání služeb dodavatelů	Organizace musí monitorovat a zkoumat kvalitu služeb od dodavatele. Zajištění je možné díky dodržování smluvních podmínek a bezpečnosti informací.
A.15.2.2	Řízení změn ve službách dodavatelů	Pokud ze strany dodavatele dochází ke změně poskytované služby, změna by měla být řízena s ohledem na kritičnost souvisejících informací a na systému v zájmu bezpečnosti informací.
A.16	**Řízení incidentů bezpečnosti informací**	
A.16.1	Řízení incidentů bezpečnosti informací a zlepšování	

A.16.1.1	Odpovědnosti a postupy	Pro zajištění rychlé, efektivní a systematické reakce na incidenty bezpečnosti informací by měly být ustanoveny odpovědnosti a postupy pro zvládání incidentů bezpečnosti informací.
A.16.1.2	Hlášení událostí bezpečnosti informací	Hlášení bezpečnostních událostí musí být učiněno bezprostředně po incidentu pomocí předurčených komunikačních kanálů.
A.16.1.3	Hlášení slabých míst bezpečnosti informací	Zaměstnanci a smluvní strany používající informační systémy a služby si musí všímat a hlásit jakákoli slabá místa bezpečnosti informací v systémech a službách.
A.16.1.4	Posouzení a rozhodnutí o událostech bezpečnosti informací	Na základě rizika a politiky se musí klasifikovat bezpečnostní incident a rozhodnout o dalším postupu.
A.16.1.5	Reakce na incidenty bezpečnosti informací	Jakákoli reakce na bezpečnostní incidenty musí být v souladu s dokumentovanými postupy.
A.16.1.6	Ponaučeni z incidentů bezpečnosti informací	Ke snížení pravděpodobnosti nebo dopadu následných incidentů se musí používat znalosti získané z analýzy a řešení incidentů bezpečnosti informací.
A.16.1.7	Shromažďování důkazů	Pro případ útoku je nutné stanovit postupy pro vytváření, shromažďování a uchovávání informací, které mohou sloužit jako důkaz pro následující právní kroky.
A.17	**Aspekty řízení kontinuity činností organizace z hlediska bezp. informací**	
A.17.1	Kontinuita bezpečnosti informací	
A.17.1.1	Plánování kontinuity bezpečnosti informací	Organizace musí naplánovat a vytvořit směrnici pro požadavky na bezpečnost informací a kontinuitu řízení bezpečnosti informací v nepříznivých situacích (krize, katastrofy, havárie).
A.17.1.2	Implementace kontinuity bezpečnost informací	Vytvořená směrnice v opatření A.17.1.1 musí být implementována.
A.17.1.3	Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací	Opatření zavedené v A.17.1.2 musí být pravidelně ověřována pro efektivnost v případe nepříznivé situace.
A.17.2	Redundance	
A.17.2.1	Dostupnost vybavení pro zpracování informací	Vybavení pro zpracování informací musí být implementováno s dostatečnou redundancí, aby byly splněny požadavky na dostupnost.
A.18	**Soulad s požadavky**	
A.18.1	Soulad s právními a smluvními požadavky	

A.18.1.1	Identifikace odpovídající legislativy a smluvních požadavků	Všechny zákonné, smluvní, předpisové požadavky příslušné legislativy a přístup organizace ke splnění těchto požadavků musí být explicitně identifikovány, dokumentovány a udržovány v aktuálním stavu pro každý informační systém a organizaci.
A.18.1.2	Ochrana duševního vlastnictví	Pro zajištění souladu s legislativními, předpisovými a smluvními požadavky týkající se práv duševního vlastnictví a používání proprietárních softwarových produktů musí být implementována vhodná opatření.
A.18.1.3	Ochrana záznamů	Záznamy organizace musí být chráněny před ztrátou, zničením, falšováním a neoprávněnému přístupu v souladu s bezpečnostními požadavky.
A.18.1.4	Soukromí a ochrana osobních údajů	Soukromí a ochrana osobních údajů musí být zajištěny v souladu s odpovídající legislativou a s předpisy, pokud je to použitelné.
A.18.2	Přezkoumání bezpečnosti informací	
A.18.2.1	Nezávislá přezkoumání bezpečnosti informací	Přístup organizace k implementaci a řízení bezpečnosti informací musí být nezávisle přezkoumáván v plánovaných intervalech nebo když nastane významná změna.
A.18.2.2	Shoda s bezpečnostními politikami a normami	Vedoucí pracovníci by měli pravidelně přezkoumávat soulad zpracování informací a postupy v rámci své působnosti s příslušnými bezpečnostními politikami, normami a jakýmikoli dalšími požadavky na bezpečnost.

PŘÍLOHA Č. 2: PROHLÁŠENÍ O APLIKOVATELNOSTI PRVNÍ ETAPY

A.5 Politiky bezpečnosti informací

A.5.1 Směřování bezpečnosti informací vedením organizace

Cíl: Určit směr a vyjádřit podporu bezpečnosti informací ze strany vedení v souladu s požadavky týkajícími se činnosti organizace, příslušnými zákony a směrnicemi.

A.5.1.1 Politiky pro bezpečnost informací

Opatření: Soubor politik pro bezpečnost informací musí být definován, schválen vedením organizace, vydán a dán na vědomí všem zaměstnancům a relevantním externím stranám.

Vyloučeno: Ne

Způsob plnění požadavku: vytvořena bezpečnostní politika

A.5.1.2 Přezkoumání politik pro bezpečnost informací

Opatření: Pro zjištění neustálé vhodnosti, přiměřenosti a efektivnosti musí být politiky pro bezpečnost informací přezkoumávány v plánovaných intervalech vždy, když nastane významná změna.

Vyloučeno: Ne

Způsob plnění požadavku: přezkoumávání vhodnosti, přiměřenosti a efektivnosti opatření po cyklech trvajících maximálně dvanáct měsíců.

A.6 Organizace bezpečnosti informací

A.6.1 Interní organizace

Cíl: Ustanovit rámec řízení pro zahájení a řízení implementace a provozování bezpečnosti informací v organizaci.

A.6.1.1 Role a odpovědnosti bezpečnosti informací

Opatření: Musí být definovány a přiděleny odpovědnosti v oblasti bezpečnosti informací.

Vyloučeno: Ne

Způsob plnění požadavku: definování odpovědností vedením organizace.

A.6.1.2 Princip oddělení povinností

Opatření: Pro snížení příležitostí k neoprávněné nebo neúmyslné modifikaci nebo zneužití aktiv organizace musí být zajištěno oddělení neslučitelných povinností a odpovědností.

Vyloučeno: Ne

Způsob plnění požadavku: Vedení organizace zajistí vytvoření dokumentu s popisem pracovních pozic (role, odpovědnosti, práva, povinnosti).

A.6.1.3 Kontakt s příslušnými orgány a autoritami

Opatření: Musí být udržovány přiměřené vztahy s příslušnými orgány a autoritami.

Vyloučeno: Ne (aktualizace)

Způsob plnění požadavku: Aktualizace seznamu využívaných kontaktů (rozšíření například o Národní úřad pro kybernetickou a informační bezpečnost) s odebíráním novinek z jejich webových stránek.

A.6.1.4 Kontakt se zájmovými skupinami

Opatření: Musí být udržovány přiměřené vztahy s odbornými zájmovými skupinami nebo ostatními odbornými fóry na bezpečnost a profesními sdruženími.

Vyloučeno: Ano

Způsob plnění požadavku: Vedení obce již zajišťuje sledování webových stránek s novinkami o kybernetické bezpečnosti.

A.6.1.5 Bezpečnost informací v řízení projektů

Opatření: Bezpečnost informací musí být zohledněna v řízení projektů nezávisle na typu projektu.

Vyloučeno: Ne

Způsob plnění požadavku: Při řízení projektů organizace využívá nejnovějších norem a doporučení v oblasti bezpečnosti informací.

A.6.2 Mobilní zařízení a práce na dálku.

Cíl: Zajistit bezpečnost při použití mobilních zařízení a pro práci na dálku.

A.6.2.1 Politika mobilních zařízení

Opatření: Musí být přijata politika a relevantní bezpečnostní opatření pro zvládání rizik spojených s používáním mobilních zařízení.

Vyloučeno: Ne

Způsob plnění požadavku: Vytvoření politik a manuálu uživatele po využívání mobilních zařízení.

A.6.2.2 Práce na dálku

Opatření: Musí být implementována politika a relevantní bezpečnostní opatření na ochranu informací, která jsou přístupná, zpracovaná nebo ukládaná v místech pro práci na dálku.

Vyloučeno: Ne

Způsob plnění požadavku: Definice požadavků na zabezpečení komunikace pro práci na dálku.

A.7 Bezpečnost lidských zdrojů

A.7.1 Před vznikem pracovního vztahu

Cíl: Zajistit, aby zaměstnanci a smluvní strany byli srozuměni se svými povinnostmi a aby pro jednotlivé role byli vybráni vhodní kandidáti.

A.7.1.1 Prověřování

Opatření: Všichni uchazeči o zaměstnání musí být prověřeni podle platných zákonů, předpisů a v souladu s etikou. Prověření musí být prováděna na základě požadavků, týkajících se činnosti organizace, dále s ohledem na klasifikaci informací, ke kterým by měli získat přístup a také z hlediska potenciálních rizik.

Vyloučeno: Ne (zavedeno)

Způsob plnění požadavku: Organizace pečlivě vybírá uchazeče přes vícekolové výběrové řízení, kdy se zjišťují dovednosti a provádí se prověrka s ohledem na klasifikaci informací budoucí pracovní pozice.

A.7.1.2 Podmínky pracovního vztahu

Opatření: Pracovní smlouvy uzavřené se zaměstnanci a smluvními stranami musí obsahovat ustanovení o jejich odpovědnostech a odpovědnostech organizace za bezpečnost informací.

Vyloučeno: Ne (zavedeno)

Způsob plnění požadavku: Definice podmínek pracovních vztahů v pracovní smlouvě.

A.7.2 Během pracovního vztahu

Cíl: Zajistit, aby si zaměstnanci a smluvní strany byli vědomi toho, že si musí plnit svoje povinnosti v oblasti bezpečnosti informací.

A.7.2.1 Odpovědnosti vedení organizace

Opatření: Vedení organizace musí po všech zaměstnancích a smluvních stranách požadovat dodržování bezpečnosti informací v souladu s ustanovenými politikami a postupy v organizaci.

Vyloučeno: Ne (aktualizovat)

Způsob plnění požadavku: Pravidelná kontrola.

A.7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací

Opatření: Všichni zaměstnanci organizace, a je-li to relevantní i smluvní strany, musí s ohledem na svou pracovní náplň dostávat odpovídající vzdělávání a školení pro zvyšování povědomí bezpečnosti informací a musí být pravidelně informováni o změnách v politikách a postupech bezpečnosti informací.

Vyloučeno: Ne

Způsob plnění požadavku: Pravidelná školení pro zvyšování kvalifikace zaměstnanců a jejich povědomí o bezpečnosti informací.

A.7.2.3 Disciplinární řízení

Opatření: Musí existovat formální proces disciplinárního řízení k přijetí opatření vůči zaměstnancům, kteří se dopustili narušení bezpečnosti informací.

Vyloučeno: Ne (aktualizovat)

Způsob plnění požadavku: Definování postupů při disciplinárním řízení.

A.7.3 Ukončení a změna pracovního vztahu

Cíl: Chránit zájmy organizace v rámci procesu změny nebo ukončení pracovního vztahu.

A.7.3.1 Odpovědnosti při ukončení nebo změně pracovního vztahu

Opatření: Odpovědnosti a povinnosti v oblasti bezpečnosti informací, které zůstávají platné po ukončení nebo změně pracovního vztahu, musí být definovány, komunikovány se zaměstnanci nebo smluvními stranami a prosazovány.

Vyloučeno: Ne (zavedeno)

Způsob plnění požadavku: Definice postupů při disciplinárních řízeních.

A.8 Řízení aktiv

A.8.1 Odpovědnost za aktiva

Cíl: Identifikovat aktiva organizace a definovat odpovědnosti k jejich přiměřené ochraně.

A.8.1.1 Seznam aktiv

Opatření: Aktiva související s informacemi a vybavení pro zpracování informací musí být identifikována a seznam těchto aktiv musí být vytvořen a udržován aktuální.

Vyloučeno: Ne (aktualizovat)

Způsob plnění požadavku: Aktualizovat dle vypracované analýzy této práce.

A.8.1.2 Vlastnictví aktiv

Opatření: Aktiva udržovaná v seznamu musí mít určeného vlastníka.

Vyloučeno: Ne (aktualizovat)

Způsob plnění požadavku: Aktualizovat podle novému seznamu aktiv.

A.8.1.3 Přípustné použití aktiv

Opatření: Musí být určena, dokumentována a implementována pravidla pro přípustné použití informací a aktiv souvisejících s informacemi a vybavením pro zpracování informací.

Vyloučeno: Ne (aktualizovat)

Způsob plnění požadavku: Vytvoření dokumentu definujícího přípustné použití všech identifikovaných aktiv.

A.8.1.4 Navrácení aktiv

Opatření: Při ukončení pracovního vztahu, smluvního vztahu nebo dohody musí zaměstnanci a pracovníci externích stran odevzdat veškerá jim svěřená aktiva, která jsou majetkem organizace.

Vyloučeno: Ne (aplikováno)

Způsob plnění požadavku: Pracovní smlouva obsahuje odstavce pro vracení aktiv po ukončení smlouvy.

A.8.2 Klasifikace informací

Cíl: Zajistit, aby informace získaly odpovídající úroveň ochrany v souladu s jejich důležitostí pro organizaci.

A.8.2.1 Klasifikace informací

Opatření: Informace musí být klasifikovány s ohledem na zákonné požadavky, jejich hodnotu, kritičnost a citlivost vůči neoprávněnému prozrazení nebo modifikaci.

Vyloučeno: Ne

Způsob plnění požadavku: Dle dokumentace ISMS.

A.8.2.2 Označování informací

Opatření: Pro označování informací musí být vytvořen a implementován vhodný soubor postupů, které budou v souladu se schématem klasifikace informací přijatým organizací.

Vyloučeno: Ne

Způsob plnění požadavku: Dle dokumentace ISMS.

A.8.2.3 Manipulaci s aktivy

Opatření: Pro manipulaci s aktivy musí být vytvořeny a implementovány postupy v souladu se schématem klasifikace informací přijatých organizací.

Vyloučeno: Ne

Způsob plnění požadavku: Dle dokumentace ISMS.

A.8.3 Manipulace s médii

Cíl: Předcházet neoprávněnému vyzrazení, modifikaci, odstranění nebo zničení informací uložených na médiích.

A.8.3.1 Správa výměnných médií

Opatření: Musí být implementovány postupy pro správu výměnných médií v souladu se schématem klasifikace informací přijatých organizací.

Vyloučeno: Ne

Způsob plnění požadavku: Definice postupů a školení zaměstnanců pro správu výměnných médií.

A.8.3.2 Likvidace médií

Opatření: Média, pokud nejsou dále upotřebitelná, musí být bezpečně zlikvidována v souladu s formalizovanými postupy.

Vyloučeno: Ne

Způsob plnění požadavku: Média jsou vyřazována z provozu úplným fyzickým zničením a při požadavku znovupoužití jsou například vícenásobně přepsány tak, aby nebyla možná rekonstrukce dat.

A.8.3.3 Přeprava fyzických médií

Opatření: Média obsahující informace musí být během přepravy chráněna proti neoprávněnému přístupu, zneužití nebo narušení.

Vyloučeno: Ne

Způsob plnění požadavku: Definice postupů ochrany médií při přepravě.

A.9 Řízení přístupu

A.9.1 Požadavky organizace na řízení přístupu

Cíl: Omezit přístup k informacím a vybavení pro zpracování informací

A.9.1.1 Politika řízení přístupu

Opatření: Musí být ustanovena, dokumentována a přezkoumávána politika řízení přístupu v závislosti na požadavcích na činnosti organizace a bezpečnosti informací.

Vyloučeno: Ne

Způsob plnění požadavku: Definice politiky řízení přístupu dle provozního řádu organizace.

A.9.1.2 Přístup k sítím a síťovým službám

Opatření: Uživatelé musí mít přístup pouze k těm sítím a síťovým službám, pro jejichž použití byli zvlášť oprávněni.

Vyloučeno: Ne

Způsob plnění požadavku: Na základě dokumentu o oprávnění a rolích jsou nastaveny přístupy uživatelům pouze k prvkům nezbytně nutným k vykonávání jejich činnosti.

A.9.2 Řízení přístupu uživatelů

Cíl: Zajistit oprávněný přístup uživatelů a předcházet neoprávněnému přístupu k systémům a službám.

A.9.2.1 Registrace a zrušení registrace uživatele

Opatření: Pro přidělování přístupových práv musí být implementován proces formalizované registrace uživatele včetně jejího zrušení.

Vyloučeno: Ne (zavedeno)

Způsob plnění požadavku: Dle provozního řádu organizace.

A.9.2.2 Správa uživatelských přístupů

Opatření: Pro přidělování a odebírání přístupových práv všem typům uživatelů ke všem systémům a službám musí být implementován formalizovaný proces správy uživatelských přístupů.

Vyloučeno: Ne (zavedeno)

Způsob plnění požadavku: Dle provozního řádu organizace

A.9.2.3 Správa privilegovaných přístupových práv

Opatření: Musí být omezeno a řízeno přidělování a používání privilegovaných přístupových práv.

Vyloučeno: Ne

Způsob plnění požadavku: Vytvoření dokumentu, který definuje správu privilegovaných přístupových práv.

A.9.2.4 Správa tajných autentizačních informací uživatelů

Opatření: Přidělování tajných autentizačních informací musí být řízeno formalizovaným procesem.

Vyloučeno: Ne

Způsob plnění požadavku: Školení dle ISMS, které obsahuje například zásady pro bezpečné heslo.

A.9.2.5 Přezkoumání přístupových práv uživatelů

Opatření: Vlastníci aktiv musí v pravidelných intervalech přezkoumávat přístupová práva uživatelů.

Vyloučeno: Ne

Způsob plnění požadavku: Vlastníci aktiv jsou zodpovědní za přezkoumávání přístupových práv ostatních uživatelů.

A.9.2.6 Odebrání nebo úprava přístupových práv

Opatření: Při ukončení nebo změně pracovního vztahu, smluvního vztahu nebo dohody musí být všem zaměstnancům a externím stranám odejmuta nebo pozměněna přístupová práva k informacím a vybavení pro zpracování informací.

Vyloučeno: Ne (zavedeno)

Způsob plnění požadavku: Pracovní smlouva obsahuje odstavec pro postupy odebírání přístupových práv při ukončení pracovního vztahu.

A.9.3 Odpovědnosti uživatelů

Cíl: Učinit uživatele odpovědné za ochranu jejich autentizačních informací

A.9.3.1 Používání tajných autentizačních informací

Opatření: Při používání tajných autentizačních informací musí být po uživatelích vyžadováno, aby dodržovali postupy stanovené organizací.

Vyloučeno: Ne

Způsob plnění požadavku: Dle pracovní smlouvy a směrnic k uživatelským účtům.

A.9.4 Řízení přístupu k systémům a aplikacím

Cíl: Předcházet neautorizovanému přístupu k systémům a aplikacím.

A.9.4.1 Omezení přístupu k informacím

Opatření: V souladu s politikou řízení přístupu musí být omezen přístup k informacím a funkcím aplikace.

Vyloučeno: Ne

Způsob plnění požadavku: Podle dokumentu s popisem pracovních pozic (role, práva, povinnosti, odpovědnosti) jsou nastaveny přístupy pomocí Group Policy (s využitím Active Directory).

A.9.4.2 Bezpečné postupy přihlášení

Opatření: Pokud to politika řízení přístupu vyžaduje, musí být přístup k systémům a aplikacím řízen postupy bezpečného přihlášení.

Vyloučeno: Ne

Způsob plnění požadavku: Školení uživatelů, manuály uživatele a manuály k jednotlivým aplikacím či službám.

A.9.4.3 Systém správy hesel

Opatření: Systémy správy hesel musí být interaktivní a musí zajišťovat použití kvalitních hesel.

Vyloučeno: Ne

Způsob plnění požadavku: Školení uživatelů, dokument pro správu hesel.

A.9.4.4 Použití privilegovaných programových nástrojů

Opatření: Musí být omezeno a přísně kontrolováno použití programových nástrojů, které mohou být schopné překonat systémové nebo aplikační kontroly.

Vyloučeno: Ano

Způsob plnění požadavku: Nejsou používány.

A.9.4.5 Řízení přístupu ke zdrojovým kódům

Opatření: Musí být omezen přístup ke zdrojovým kódům programů.

Vyloučeno: Ano

Způsob plnění požadavku: Uživatelé organizace nemají možnost se dostat ke zdrojovým kódům programů.

A.10 Kryptografie

A.10.1 Kryptografická opatření

Cíl: Zajistit řádné a efektivní používání kryptografie k ochraně důvěrnosti, autentičnosti a integrity informací.

A.10.1.1 Politika pro použití kryptografických opatření

Opatření: Musí být vytvořena a implementována politika pro užívání kryptografických opatření na ochranu informací.

Vyloučeno: Ne

Způsob plnění požadavku: Vytvoření dokumentu definujícího postupy pro kryptografii, vybrání nástroje pro šifrování.

A.10.1.2 Správa klíčů

Opatření: Politika pro používání, ochranu a dobu existence kryptografických klíčů musí být vytvořena a implementována po celou dobu jejich životního cyklu.

Vyloučeno: Ne

Způsob plnění požadavku: Dle provozního řádu organizace.

A.11 Fyzická bezpečnost a bezpečnost prostředí

A.11.1 Bezpečnost oblasti

Cíl: Předcházet neautorizovanému fyzickému přístupu, poškození a zásahům do informací a vybavení pro zpracování informací organizace.

A.11.1.1 Fyzický bezpečnostní perimetr

Opatření: Bezpečnostní perimetry musí být definovány a používány k ochraně oblastí, které obsahují citlivé nebo kritické informace a vybavení pro zpracování informací.

Vyloučeno: Ne (aktualizovat)

Způsob plnění požadavku: Revize a vylepšení jednotlivých aspektů zabezpečení fyzického perimetru (lepší zámky na dveře, bezpečnostní dveře, atd).

A.11.1.2 Fyzické kontroly vstupu

Opatření: Aby bylo zajištěno, že je přístup do bezpečných oblastí povolen pouze oprávněným osobám, musí být tyto oblasti chráněny vhodným systémem vstupních kontrol.

Vyloučeno: Ne (zavedeno)

Způsob plnění požadavku: Kontrola u sekretářky a za pomocí elektronické autentizace při vstupu do budovy.

A.11.1.3 Zabezpečení kanceláří, místností a vybavení

Opatření: Musí být navržena a aplikována fyzická bezpečnost kanceláří, místností a vybavení.

Vyloučeno: Ne (zavedeno)

Způsob plnění požadavku: Je aplikovaná fyzická bezpečnost kanceláří (zámky, kamery, evidence klíčů, atd).

A.11.1.4 Ochrana před vnějšími hrozbami a hrozbami prostředí

Opatření: Musí být navržena a aplikována fyzická ochrana proti přírodním katastrofám, úmyslnému útoku nebo haváriím.

Vyloučeno: Ne (zavedeno)

Způsob plnění požadavku: Dle technických možností (kamerový systém, kontroly vstupu, mříže na oknech, havarijní plány pro případ havárie).

A.11.1.5 Práce v bezpečných oblastech

Opatření: Musí být navrženy a aplikovány postupy pro práci v bezpečných oblastech.

Vyloučeno: Ano

Způsob plnění požadavku: Neprovádí se.

A.11.1.6 Oblasti pro nakládku a vykládku

Opatření: Přístupové body, jako oblasti pro nakládku a vykládku a další místa, kde se mohou neoprávněné osoby dostat do prostorů organizace, musí být kontrolovány a pokud je to možné, jsou izolovány od vybavení pro zpracování informací, aby se zabránilo neoprávněnému přístupu k nim.

Vyloučeno: Ano

Způsob plnění požadavku: Nepoužívají se.

A.11.2 Zařízení

Cíl: Předcházet ztrátě, poškození, krádeži nebo kompromitaci aktiv a přerušení činností organizace.

A.11.2.1 Umístění zařízení a jeho ochrana

Opatření: Zařízení musí být umístěna a chráněna tak, aby se snížila rizika hrozeb a nebezpečí daná prostředím a aby se omezily příležitosti pro neoprávněný přístup.

Vyloučeno: Ne (aktualizovat)

Způsob plnění požadavku: Fyzické zabezpečení kanceláří a archivu, využívání hostingových center nebo využití nejvíce zabezpečených částí budovy.

A.11.2.2 Podpůrné služby

Opatření: Zařízení musí být chráněno před selháním napájení a před dalšími výpadky způsobenými selháním podpůrných služeb.

Vyloučeno: Ne (aktualizovat)

Způsob plnění požadavku: Zřízení redundantního internetového připojení, údržba a včasná výměna zdroje nepřerušovaného napětí.

A.11.2.3 Bezpečnost kabelových rozvodů

Opatření: Silové a telekomunikační kabelové rozvody, které jsou určeny pro přenos dat nebo podporu informačních služeb, musí být chráněny před odposlechem, rušením či poškozením

Vyloučeno: Ne (aktualizovat)

Způsob plnění požadavku: Správné technické řešení budovy, kabelážní lišty, omezený přístup k rozvaděčům a kabelovým trasám, monitoring výpadků.

A.11.2.4 Údržba zařízení

Opatření: Zařízení musí být správně udržováno pro zajištění jeho stálé dostupnosti a integrity.

Vyloučeno: Ne (aktualizovat)

Způsob plnění požadavku: Definovány povinnosti související s údržbou konkrétních zařízení (jednotlivým uživatelům nebo třetí straně).

A.11.2.5 Přemístění aktiv

Opatření: Zařízení, informace nebo software nesmí být přemísťovány mimo prostory organizace bez předchozího schválení.

Vyloučeno: Ne

Způsob plnění požadavku: Definice přemisťování aktiv mimo prostory organizace (vždy musí být projednána a schválena s vedením organizace).

A.11.2.6 Bezpečnost zařízení a aktiv mimo prostory organizace

Opatření: Aktiva mimo prostory organizace musí být zabezpečena s přihlédnutím k rozdílným rizikům, která vyplývají z jejich použití mimo organizaci.

Vyloučeno: Ne

Způsob plnění požadavku: Definice zabezpečení a nakládání s aktivy mimo prostory organizace.

A.11.2.7 Bezpečná likvidace nebo opakované použití zařízení

Opatření: Všechny prvky zařízení, obsahující paměťová média, musí být zkontrolovány tak, aby bylo zajištěno, že před jejich likvidací nebo opakovaným použitím budou jakákoliv citlivá data a licencovaný software odstraněny nebo bezpečně přepsány.

Vyloučeno: Ne

Způsob plnění požadavku: Znehodnocuje se buď úplným fyzickým zničením nebo v případě znovu používání zařízení například vícenásobným nulovým přepisem (data nejdou zrekonstruovat).

A.11.2.8 Uživatelská zařízení bez obsluhy

Opatření: Uživatelé musí zajistit přiměřenou ochranu zařízení bez obsluhy.

Vyloučeno: Ne

Způsob plnění požadavku: Směrnice pro správnou obsluhu zařízení.

A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru

Opatření: Musí být přijata zásada prázdného stolu ve vztahu k dokumentům a výměnným paměťovým médiím a zásada prázdné obrazovky monitoru u vybavení pro zpracování informací.

Vyloučeno: Ne

Způsob plnění požadavku: Směrnice pro správnou obsluhu zařízení (například nastavení uzamykání operačního systému), uzamykací zásuvky v pracovních stolech.

A.12 Bezpečnost provozu

A.12.1 Provozní postupy a odpovědnosti

Cíl: Zajistit správný a bezpečný provoz vybavení pro zpracování informací.

A.12.1.1 Dokumentované provozní postupy

Opatření: Provozní postupy musí být dokumentovány a musí být dostupné uživatelům podle potřeby.

Vyloučeno: Ne

Způsob plnění požadavku: Definice dokumentace provozních postupů a prací s nimi.

A.12.1.2 Řízení změn

Opatření: Změny v organizaci a jejích procesech, v prostředích pro zpracování informací a systémech, které ovlivňují bezpečnost informací, musí být řízeny.

Vyloučeno: Ne

Způsob plnění požadavku: Vedení zajistí kontrolu a řízení změn v organizaci a jejích procesech (například v provozním řádu).

A.12.1.3 Řízení kapacit

Opatření: Pro zajištění požadovaného výkonu systému, s ohledem na budoucí kapacitní požadavky, musí být monitorováno, nastaveno a předvídáno využití zdrojů.

Vyloučeno: Ne

Způsob plnění požadavku: Dohled nad vytížeností lidských zdrojů a ICT.

A.12.1.4 Princip oddělení prostředí vývoje, testování a provozu

Opatření: Pro snížení rizika neoprávněného přístupu nebo změn provozního prostředí musí být odděleno prostředí vývoje, testování a provozu.

Vyloučeno: Ano

Způsob plnění požadavku: Nevztahuje se na organizaci.

A.12.2 Ochrana proti malwaru

Cíl: Zajistit, aby informace a vybavení pro zpracování informací byly chráněny proti malwaru.

A.12.2.1 Opatření proti malwaru

Opatření: Na ochranu proti malwaru musí být implementována opatření na jeho detekci, prevenci a obnovu, a to ve spojení s odpovídajícím bezpečnostním povědomím uživatelů.

Vyloučeno: Ne (zavedeno)

Způsob plnění požadavku: Organizace využívá antivir a firewall vestavěný do routeru a operačního systému, zálohování dat.

A.12.3 Zálohování

Cíl: Chránit proti ztrátě dat.

A.12.3.1 Zálohování informací

Opatření: Záložní kopie informací, softwaru a binárních obrazů systému musí být pořizovány v pravidelných intervalech v souladu se schválenou politikou zálohování.

Vyloučeno: Ne (aktualizovat)

Způsob plnění požadavku: Vytvoření směrnice na zálohování dat (co zálohovat, kam zálohovat, jak často zálohovat, jak šifrovat, atd).

A.12.4 Zaznamenávání formou logů a monitorování

Cíl: Zaznamenávat události a vytvářet záznamy

A.12.4.1 Zaznamenávání událostí formou logů

Opatření: Musí být pořizovány, uchovávány a pravidelně přezkoumávány logy událostí zaznamenávající aktivity uživatelů, výjimky, selhání a události bezpečnosti informací.

Vyloučeno: Ne

Způsob plnění požadavku: Koupě softwaru a hardwaru na záznam logů, určení osoby, která bude logy zpracovávat.

A.12.4.2 Ochrana logů

Opatření: Prostředky pro zaznamenávání formou logů a logy musí být chráněny proti zfalšování a neoprávněnému přístupu.

Vyloučeno: Ne

Způsob plnění požadavku: Součástí zálohování a přidělení přístupů.

A.12.4.3 Logy o činnosti administrátorů a operátorů

Opatření: Aktivity systémového administrátora a systémového operátora musí být logovány a logy chráněny a pravidelně přezkoumávány.

Vyloučeno: Ne

Způsob plnění požadavku: Pravidelné přezkoumávání logů aktivit systémového administrátora a osoby, která se stará o zpracování logů.

A.12.4.4 Synchronizace hodin

Opatření: Hodiny všech důležitých systémů pro zpracování informací musí být v rámci organizace nebo bezpečnostních domén synchronizovány s jediným referenčním zdrojem času.

Vyloučeno: Ne

Způsob plnění požadavku: Seřízení hodin důležitých systémů dle externího zdroje (světové atomové hodiny).

A.12.5 Správa provozního softwaru

Cíl: Zajistit integritu provozních systémů

A.12.5.1 Instalace softwaru na provozní systémy

Opatření: Musí být implementovány postupy řízené instalace softwaru na provozních systémech.

Vyloučeno: Ne

Způsob plnění požadavku: Definice postupů instalace softwarů na provozní systémy.

A.12.6 Řízení technických zranitelností

Cíl: Zabránit využívání technických zranitelností.

A.12.6.1 Řízení technických zranitelností

Opatření: Musí být zajištěno včasné získání informací o existenci technických zranitelností provozovaných informačních systémů, vyhodnocena úroveň ohrožení organizace vůči těmto zranitelnostem a přijata příslušná opatření na zvládání souvisejících rizik.

Vyloučeno: Ne

Způsob plnění požadavku: redundance, monitorování provozu v systému.

A.12.6.2 Omezení instalace softwaru

Opatření: Musí být ustanovena a implementována pravidla ohledně instalace softwaru uživateli.

Vyloučeno: Ne (aktualizovat)

Způsob plnění požadavku: Omezeny přístupy jednotlivých uživatelů, školení.

A.12.7 Hlediska auditu informačních systémů

Cíl: Minimalizovat dopady auditních činností na provozní systémy.

A.12.7.1 Opatření k auditu informačních systémů

Opatření: Požadavky auditu a činnosti zahrnující verifikaci provozních systémů musí být pečlivě naplánovány a schváleny, aby se minimalizovalo narušení procesů organizace.

Vyloučeno: Ano

Způsob plnění požadavku: Organizace neprovádí úplné audity, částečné audity si provádí svépomocí.