

***Projektová dokumentace***

***„Vybudování JCE IB SOŠ INFORMATIKY A SPOJŮ A SOU  
KOLÍN - zpracování projektové dokumentace“***

***TECHNOLOGICKÁ ČÁST JCE IB***

***D.1.4.9. Technologie a řešení JCE IB***

***D.1.4.9.20. ORGANIZAČNÍ OPATŘENÍ***

**Zpracoval:**

Petr Lacina

## 20 ORGANIZAČNÍ OPATŘENÍ - ŠKOLA

### 20.1 NÁVRH ŘEŠENÍ

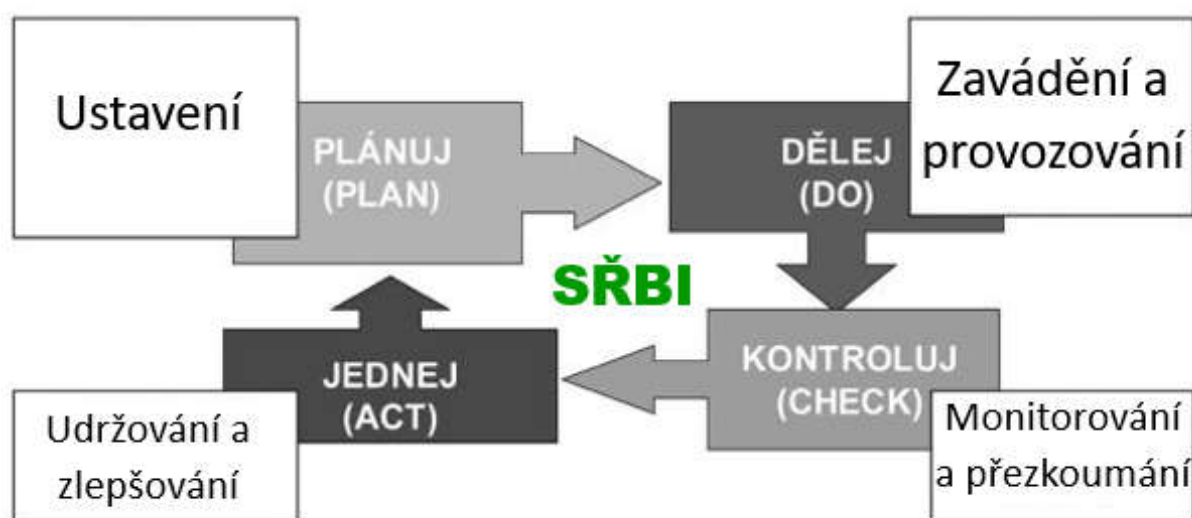
Bezpečnostním opatřením se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru (ZoKB<sup>1</sup>, §4, odst. 1). Z této definice vyplývá, že bezpečnostní opatření jsou realizována kombinací opatření organizačních a technických a že jejich cílem je zajištění jak ochrany aktiv, tak i kontinuity byznysu organizace.

#### 20.1.1 Organizační opatření

Pro zajištění ustavení, zavedení, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací a dat je nezbytné učinit patřičné kroky. To je také jasně definováno ve VyKB<sup>2</sup> § 2

j) systémem řízení bezpečnosti informací část systému řízení povinné osoby založená na přístupu k rizikům informačního a komunikačního systému, která stanoví způsob ustavení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací a dat.

### Demingův cyklus (PDCA)



V opatřeních ID 1-10 Studie – Metodické posouzení podle MBS<sup>3</sup> jsou uvedena mimo nálezu a komentáře i doporučení, jak identifikované neshody řešit. Organizační opatření je dále nutné zavádět i ve vazbě na opatření technická – viz Studie ID 11 - 18.

<sup>1</sup> Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

<sup>2</sup> Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti

<sup>3</sup> MBS – Minimální bezpečnostní standard NÚKIB

**Organizační opatření je možné v organizaci Zadavatele variantně řešit:**

1. pouze vlastními silami (bez vynaložení přímých finančních prostředků, je ale nutné značné úsilí Zadavatele),
2. vlastními silami Zadavatele s podporou konzultanta Řešitele (zde záleží jaký čas bude potřebný na zajištění konzultační podpory s tím, že běžná cena IB/KB konzultanta se pohybuje v sazbě cca 1500,- Kč/h bez DPH),
3. výhradně formou dodávky externím subjektem (Zadavatel musí vynaložit potřebnou součinnost Řešiteli a zaplatit cenu za jím poskytnuté služby).

**Varianta č. 1** je bez dalších nákladů, nicméně s delší časovou náročností a s případnými náklady na dozdělení dotčených osob v oblasti KB – viz kapitola 11.2. Studie.

**Varianta č. 2** již vyžaduje spolupráci specialisty/konzultanta s finanční náročností dle jeho časového rámce, který bude potřebný. Míra jeho spoluúčasti je závislá na požadavcích ze strany Zadavatele. Osoby jednající s tímto konzultantem by měly projít vzděláváním – viz kapitola 11.2. Studie.

**Varianta č. 3** je komplexním řešením ze strany specializované poradenské firmy. V níže uvedené tabulce je uvedena souhrnná kalkulace. Jedná se o odhad s ohledem na požadavky MBS, charakteru organizace Zadavatele (Škola) a s ohledem na výsledky posouzení. Poslední položkou tabulky je cena za 1MD<sup>4</sup> práce konzultanta v oblasti IB/KB.

***20.1.1.1 Navrhované bezpečnostní politiky a bezpečnostní dokumentace***

SŘBI je systémem dokumentovaným. Pokud chci něco řídit, musím to i měřit. Tedy mít nejen vytvořeny potřebné předpisy (pravidla), ale i dokumentaci a záznamy (evidence – neboli důkazy) o provozování SŘBI. Níže jsou tedy uvedeny jak bezpečnostní politiky, tak i potřebná bezpečnostní dokumentace. Zatímco bezpečnostní politiky může za součinnosti Zadavatele vytvářet Řešitel, u bezpečnostní dokumentace je nezbytná vyšší míra aktivity na Zadavateli a jeho pracovnících.

***20.1.1.1.1 Bezpečnostní politiky***

Základním předpokladem pro zavedení informační a kybernetické bezpečnosti je nezbytnost zpracování bezpečnostních politik v následujícím členění. Při tvorbě bezpečnostních politik Řešitelem pro organizaci Zadavatele je ovšem potřebná součinnost ze strany Zadavatele z důvodu úzké vazby vytvářených předpisů na organizaci Zadavatele a z důvodu potřeby zajištění integrace SŘBI do procesů organizace Zadavatele.

Míru potřebné součinnosti Zadavatele určuje při tvorbě bezpečnostních politik vždy a výhradně Řešitel, který v těchto předpisech kombinuje svoje znalosti a know-how s informacemi o organizaci Zadavatele.

- 1) Politika organizační bezpečnosti
  - a. Určení bezpečnostních rolí a jejich práv a povinností
- 2) Politika řízení informací
  - a. Identifikace, hodnocení a evidence informací
  - b. Pravidla ochrany jednotlivých úrovní informací
  - c. Způsoby spolehlivého mazání nebo ničení technických nosičů dat, informací, provozních údajů a jejich kopií
  - d. Pravidla a postupy pro ochranu předávaných informací
  - e. Způsoby ochrany elektronické výměny informací
  - f. Pravidla pro využívání kryptografické ochrany
- 3) Politika řízení dodavatelů

---

<sup>4</sup> MD – Man Day – den práce

- a. Náležitosti smlouvy o úrovni služeb a způsobů a úrovni realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti
- b. Pravidla pro provádění kontroly zavedení bezpečnostních opatření u dodavatele
- 4) Politika bezpečnosti lidských zdrojů**
  - a. Pravidla rozvoje bezpečnostního povědomí a způsoby jeho hodnocení
  - b. Bezpečnostní školení nových zaměstnanců
  - c. Pravidla pro řešení případů porušení bezpečnostní politiky
  - d. Pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice
- 5) Politika řízení změn**
  - a. Způsob a principy řízení změn v procesech a informačních nebo komunikačních systémech
- 6) Politika řízení kontinuity činností**
  - a. Práva a povinnosti zúčastněných osob
  - b. Cíle řízení kontinuity činností
  - c. Určení a obsah potřebných plánů kontinuity činností a havarijních plánů
- 7) Politika řízení dokumentace**
- 8) Politika fyzické bezpečnosti**
  - a. Pravidla pro ochranu objektů
  - b. Pravidla pro kontrolu vstupu osob
  - c. Pravidla pro ochranu zařízení
  - d. Detekce narušení fyzické bezpečnosti
- 9) Politika řízení provozu a komunikací**
  - a. Postupy bezpečného provozu
  - b. Požadavky a standardy bezpečného provozu
- 10) Politika řízení přístupu**
  - a. Princip minimálních oprávnění/need-to-know
  - b. Požadavky na řízení přístupu
  - c. Životní cyklus řízení přístupu
  - d. Řízení privilegovaných oprávnění
  - e. Řízení přístupu pro mimořádné situace
  - f. Pravidelné přezkoumání přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách
- 11) Politika bezpečného chování uživatelů**
  - a. Pravidla pro bezpečné nakládání s informacemi
  - b. Bezpečné použití přístupového hesla
  - c. Bezpečné použití elektronické pošty a přístupu na internet
  - d. Bezpečný vzdálený přístup
  - e. Bezpečné chování na sociálních sítích
  - f. Bezpečnost ve vztahu k mobilním zařízením
- 12) Politika zálohování a obnovy a dlouhodobého ukládání**
  - a. Pravidla a postupy pro zálohování a obnovu
- 13) Politika řízení technických zranitelností**
- 14) Politika bezpečného používání mobilních zařízení**
- 15) Politika akvizice, vývoje a údržby**
  - a. Bezpečnostní požadavky pro akvizici, vývoj a údržbu
  - b. Řízení zranitelností
  - c. Politika poskytování a nabývání licencí programového vybavení a informací
- 16) Politika zvládání kybernetických bezpečnostních incidentů**
  - a. Pravidla a postupy pro identifikaci, evidenci a zvládání jednotlivých kategorií kybernetických bezpečnostních incidentů

- b. Pravidla a postupy pro vyhodnocení kybernetických bezpečnostních incidentů a pro zlepšování kybernetické bezpečnosti
- c. Evidence incidentů

#### *20.1.1.1.2 Doporučená bezpečnostní dokumentace*

SŘBI je dokumentovaným systémem. Proto v návaznosti na bezpečnostní politiky musí Zadavatel vytvořit i bezpečnostní dokumentaci v následujícím členění:

- 1) Plán zavádění bezpečnostních opatření
  - a. Popis bezpečnostních opatření, osoby odpovědné za zavedení jednotlivých bezpečnostních opatření, potřebné zdroje a termíny
- 2) Síťová topologie
- 3) Přehled používaných zařízení
- 4) Zprávy z auditu

Při zpracování bezpečnostní dokumentace může Zadavatel využít konzultačních služeb Řešitele. Míru využití konzultačních služeb si řídí po konzultaci s Řešitelem Zadavatel. Z tohoto důvodu nebude v kalkulaci naceněna cena konzultací jako celek, ale pouze cena za MD konzultanta.

#### *20.1.1.2 Registr zpracování osobních údajů*

SŘBI je dokumentovaným systémem. To platí i v oblasti zpracování osobních údajů. V souladu s GDPR<sup>5</sup> vyplývá pro organizaci Zadavatele povinnost řídit se požadavky, které toto nařízení na organizaci Zadavatele klade. Mimo jiné musí Zadavatel provádět záznamy o činnostech zpracování osobních údajů v souladu s článkem 30 GDPR.

### **Článek 30**

Záznamy o činnostech zpracování

- 1. Každý správce a jeho případný zástupce vede záznamy o činnostech zpracování, za něž odpovídá. Tyto záznamy obsahují všechny tyto informace:
  - a) jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů;
  - b) účely zpracování;
  - c) popis kategorií subjektů údajů a kategorií osobních údajů;
  - d) kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích;
  - e) informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce doložení vhodných záruk;
  - f) je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů;
  - g) je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1.

---

<sup>5</sup> GDPR - NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

Při tvorbě registru zpracování osobních údajů Řešitelem je nezbytná součinnost ze strany Zadavatele z důvodu zpracování osobních údajů v organizaci Zadavatele. Míru součinnosti určuje Řešitel.

#### *20.1.1.3 Zajištění kontinuity činností pro 7 identifikovaných klíčových IS organizace Zadavatele*

Pro organizaci Zadavatele je nezbytné zajištění bezpečnosti informací a služeb, které jsou poskytovány či zpracovávány jeho informačními či komunikačními systémy. Bezpečnost informací ve smyslu zajištění důvěrnosti, integrity a dostupnosti je řešena organizačními a technickými opatřeními. Zajištění nepřetržitého provozování těchto informačních systémů je nezbytné z pohledu business kontinuity organizace Zadavatele. Je tedy nezbytné zmapovat tyto klíčové IS a následně se zamyslet nad zajištěním kontinuity činností při nežádoucích či havarijních situacích.

Pro každý klíčový IS je nezbytné vytvořit evidenční list IS v rozsahu nejméně:

- Evidenční popis IS (název, verze, výrobce, podpora, garant, provozovatel, frekvence aktualizace zpracovávaných dat, veřejný/neveřejný, pořizovací náklady, roční provozní náklady)
- Účel IS
- Popis a blokové schéma IS
- Technické a programové prostředky pro zajištění provozu IS
- Způsob zajištění autentizace uživatelů a řízení přístupu
- Popis síťových technologií IS
- Způsob zaznamenávání činností v IS
- Způsob ochrany IS před škodlivým kódem
- Kryptografické prostředky
- Způsob zajištění úrovně dostupnosti IS
- Realizace vazeb IS s IS jiných správců a provozovatelů
- Současný stav IS
- Předpokládané změny v IS

Tyto evidenční listy vytváří (pokud neexistují) Zadavatel. V případě potřeby může využít služeb konzultanta v ceně dle počtu čerpaných hodin za konzultace – viz ceník níže.

V návaznosti na tyto evidenční listy IS pak Řešitel zpracuje Plány kontinuity činností (BCP). Pro každý IS zpracuje Řešitel jeden plán kontinuity činností řešící recovery proces dat pro daný IS (viz vzorový formulář níže). Tzn. bude se jednat o případ kompletní ztráty dat např. v důsledku ransomware útoku. Zadavatel poskytne Řešiteli potřebnou součinnost.

## 20.2 VZOROVÝ PLÁN KONTINUITY ČINNOSTÍ

PLÁN KONTINUITY ČINNOSTÍ (BCP)		
Hrozba	Přívalová povodeň	
Nebezpečí	Zničení serverovny, ztráta dat.	
Pravděpodobnost vzniku	střední	
OPATŘENÍ		
Prevence		
1. Umístění serverovny do vyšších pater budovy.		
2. Vytvoření záloh.		
3. Nasmalování záložní lokality. V případě vzniku mimořádné události převedení provozu informačního nebo komunikačního systému do alternativní (záložní) lokality.		
Činnosti v případě aktivace zdroje hrozby		
Scénář pokrývá nejhorší variantu, kdy bude nutné opustit budovu společnosti, ve které je uložena serverovna. V rámci testování i v průběhu ostrého nasazení plánu protiopatření musí být veškeré činnosti obnovy dokumentovány, aby mohly být zde uvedené postupy obnovy případně aktualizovány nebo upřesněny – provádí určený člen týmu.		Doba trvání
1. Svolání krizového štábu společnosti - Svolání krizového týmu IT. - Postup dle povodňového plánu společnosti. - Rozhodnutí o aktivaci záložní lokality.		2 hod
2. Zahájení přípravy spuštění záložní lokality - Sbalení vytvořených záloh na základě DRP. - Přesun odpovědných osob do záložní lokality – pracovníci odboru IT, a další členové týmu potřební pro zachování chodu nezbytných činností společnosti. - Aplikace opatření pro minimalizaci škod. - Evakuace zbytku osob a nařízení útlumové činnosti. - Instalace a konfigurace serverů, aplikací, síťových prvků na základě DRP.		5 hod
3. Zahájení ostrého provozu v záložní lokalitě Informování vedení společnosti o obnovení dostupnosti aplikací v záložní lokalitě. 2 hod.		2 hod
Konec (Celková doba trvání)		9 hod
Doporučení pro méně závažný vývoj situace		
V případě, že se krizový štáb rozhodne neaktivovat záložní lokalitu, bude utlumena činnost organizace, budou podniknuta opatření pro minimalizaci škod (protipovodňová opatření), všechny osoby budou evakuovány.		
Další postup		
Mimořádná událost bude nadále monitorována. Po opadnutí povodně začnou likvidační práce a obnovení činností organizace v plném rozsahu.		