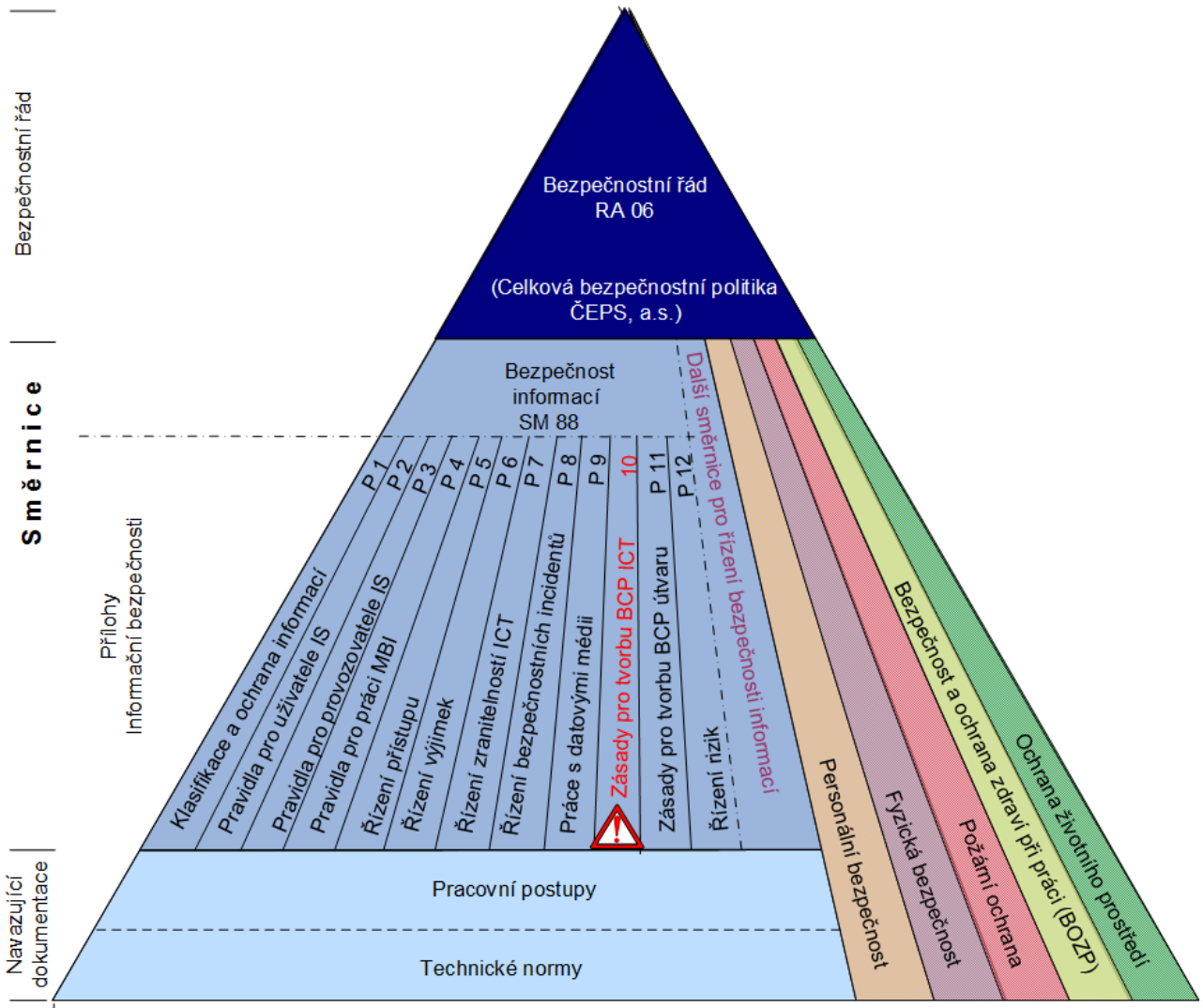
ZÁSADY PRO VYTVOŘENÍ PLÁNŮ KONTINUITY A OBNOVY ICT

Zařazení a působnost dokumentu ve struktuře bezpečnostní dokumentace



dokument / působnost	Klasifikace a ochrana informací	Pravidla pro uživatele IS	Pravidla pro provozovatele IS	Pravidla pro práci MBI	Řízení přístupu	Řízení výjimek	Řízení zranitelností ICT	Řízení bezp. incidentů	Práce s datovými médii	Zásady pro tvorbu BCP ICT	Zásady pro tvorbu BCP útvaru	Řízení rizik
uživatel IS	X	X										
provozovatel IS	X	X	X	X	X		X	X	X	X		X
MBI	X	X		X	X	X	X	X	X	X	X	X
vedoucí útvaru	X	X									X	X
personalista	X	X			X							
externí subjekt	X	X	X*)		X*)							

*) *Platí pro externí subjekty v roli správců/administrátorů/vývojářů IS*

Pozn.: Uvedené názvy nejsou přesnými názvy příloh.

OBSAH:

1 ÚČEL A PŮSOBNOST

Zásady pro vytvoření plánu kontinuity a obnovy ICT jsou přílohou směrnice *Bezpečnost informací* (dále jen „SM/88“) a obsahují zásady a principy tvorby plánů kontinuity a obnovy pro oblast informačních a komunikačních technologií (dále také havarijní plány ICT). Zásady jsou vhodným průvodcem pro tvůrce a testery plánů kontinuity a obnovy ICT.

Plán kontinuity a obnovy ICT je dokument, který popisuje, jak zachovat nebo obnovit fungování informačního nebo komunikačního systému, který byl zasažen havárií (mimořádnou událostí).

- plán je tvořen sadou postupů, doporučení a informací podle kterých bude v případě vzniku havarijní situace (mimořádné události) postupováno
- plány kontinuity a obnovy ICT (havarijní plány ICT) jsou vytvářeny pro všechny systémy, které jsou v rámci BIA identifikovány jako klíčové nebo podpůrné pro zajištění důležitých činností společnosti
- součástí životního cyklu havarijního plánu je jeho vypracování, otestování, revize a aktualizace - popis a doporučení k jednotlivým činnostem je předmětem této metodiky.

Vývoj a implementace plánů kontinuity a obnovy je nedílnou součástí procesu řízení kontinuity činností (Business Continuity Management, BCM). Realizace BCM v prostředí společnosti je v souladu s doporučeními dvojice mezinárodních norem ISO 22301, ISO 22313 která poskytuje doporučení a požadavky pro oblast řízení kontinuity činností organizace, včetně požadavků pro proces BCMS (systém řízení kontinuity činností společnosti) a jeho certifikaci.

1.1 Proces řízení kontinuity činností

Obsahem BCM je zajištění připravenosti na mimořádné události a přijetí plánovaných a nacvičených kroků k ochraně činností společnosti. V podmínkách ČEPS může být ohrožena schopnost zajistit veškeré relevantní prvky kritické infrastruktury a tím i poskytování služby přenosové soustavy, a to jak na národní tak i na evropské úrovni.

2 TERMINOLOGIE

BCM	*Business Continuity Management* - řízení kontinuity činností organizace je řídící proces podporovaný vedením společnosti, který identifikuje potenciální dopady ztrát a jehož cílem je vytvořit takové postupy a prostředí, které umožní zajistit kontinuitu a obnovu klíčových procesů a činností organizace, na předem stanovené minimální úrovni, v případě jejich narušení nebo ztráty. BCM ochraňuje zájmy klíčových podílníků, akcionářů a dalších zájmových skupin, dobrou pověst, značku společnosti. [Pojem definuje norma BS 25999-1:2006 *Business continuity management – Part 1: Code of practice.*]
BIA	Business Impact Analysis – analýza dopadů, analýza, jejímž prostřednictvím organizace kvantitativně (např. finanční ztráta, úroveň poskytovaných služeb) a kvalitativně (např. provozní, renomé, právní, regulační) zhodnotí dopady a ztráty, které mohou nastat v případě závažného incidentu, a minimální úroveň zdrojů potřebných pro obnovení kritických činností.
ISO 22301 ISO 22313	Dvojice norem poskytujících doporučení a požadavky pro oblast řízení kontinuity organizace. ISO 22301:2012 *Societal security – Business Continuity Management Systems – Requirements* je mezinárodní standard pro certifikaci systémů řízení kontinuity činností (BCMS). Specifikuje požadavky pro plánování, ustavení, zavedení, provozování, monitorování, udržování a trvalé zlepšování dokumentovaného systému připravenosti na mimořádné události. ISO 22313:2013 *Societal security – Business Continuity Management Systems – Guidance* poskytuje kritéria a doporučení dobré praxe pro účinné a objektivní řízení kontinuity organizace.
MU	*Mimořádná událost* - je incident, který svými dopady může vést až k narušení nebo přerušení činností organizace a vzniku havarijní či krizové situace.
RPO	*Recovery Point Objective* - je „bod v čase“, ke kterému je nutné zajistit obnovu dat a informací, aby bylo možné znovu zprovoznit dodávku produktu nebo služby po výpadku. Jedná se tedy o velikost zálohovací periody pro daný produkt nebo službu.

RTO	*Recovery Time Objective* - je čas stanovený pro obnovu dodávky daného produktu nebo službu na minimální přijatelné úrovni funkčnosti. Těchto časů může být v rámci analýzy dopadů (BIA) stanoveno více. Tyto hodnoty jsou vstupními parametry při určování strategie obnovy.
LBC	*Level of Business Continuity* - je údaj, který udává jaká úroveň obnovy je po přerušení dodávky požadována. Tento parametr má přímou souvislost s parametrem RTO Parametrů LBC může být pro jednu službu nebo produkt stanoveno více.

3 ROLE A ODPOVĚDNOSTI

Havarijní tým je skupinou zaměstnanců, jejichž společným cílem je vyvíjet činnosti podle předem definovaných úkolů a postupů uvedených v plánu, vztahujících se k řešení vzniklé havarijní situace a obnově funkčnosti a dostupnosti systému, který je předmětem konkrétního plánu.

Posláním členů týmu je plnit úkoly vyplývající z jednotlivých krizových scénářů (viz kapitola 7), které jsou detailně popsány v plánech. Hlavním cílem havarijního týmu je dosáhnout v požadovaném čase obnovení funkčnosti a dostupnosti systému.

Každý systém (jako např.: TRIS, DamasEnergy, ICT služby, ŘS stanic PS) má svůj havarijní tým, který je sestaven ze zaměstnanců provozních sekcí ICT (provozovatelů IS).

Vedoucí jednotlivých havarijních týmů jsou jmenováni příslušným členem představenstva pověřeným řízením úseku *Dispečerské řízení a ICT* nebo *Řízení společnosti a energetického majetku*. V kompetenci vedoucích jednotlivých týmů je vybrat a nominovat ostatní členy týmu tak, aby byly pokryty požadované dovednosti, odborné znalosti a potřeby týmu.

V následující tabulce je uveden doporučený minimální seznam rolí havarijního týmu, spolu se základními odpovědnostmi. Dle potřeby může být pro konkrétní systém počet rolí nebo členů týmu upraven.

Role	Hlavní odpovědnost
Manažer bezpečnosti informací (MBI)	• iniciuje činnosti přípravy, testování, revize a aktualizace havarijních plánů • z metodického hlediska posuzuje a připomínkuje vypracované plány kontinuity a obnovy ICT • iniciuje přípravu harmonogramu a testování plánů jednotlivých systémů • účastní se testování plánů v roli pozorovatele • s ohledem na výsledky testů dává doporučení na změny a doplnění plánů
Vedoucí týmu *(roli zastává 1 zaměstnanec)*	• odpovídá za vypracování havarijního plánu systému • vyhlašuje aktivaci plánu obnovy systému na základě vlastního zhodnocení situace • podává informace vedení o průběhu a řešení nastalé havarijní situace, a to v počáteční fázi několikrát denně, v jejím dalším průběhu pak minimálně 1x za den • řídí a koordinuje všechny činnosti zvládání havarijní situace a obnovy dostupnosti systému • odpovídá za zajištění prostředků a podmínek práce členů týmu po celou dobu aktivace havarijního plánu • musí mít přehled o všech činnostech, které je potřebné v rámci obnovení dostupnosti systému vykonat, zejména z hlediska jejich kapacitních požadavků a časové náročnosti • odpovídá za sestavení harmonogramu pravidelného testování havarijních plánů • odpovídá za pravidelnou revizi, aktualizaci a testování havarijních plánů

	• odpovídá za distribuci aktuálních verzí havarijních plánů • odpovídá za proškolování zaměstnanců v nezbytném rozsahu • výsledky testů havarijních plánů předkládá řediteli příslušné sekce ICT a manažerovi bezpečnosti informací,
Zástupce vedoucího týmu *(roli zastává 1 zaměstnanec)*	• vykonává úkoly dle pokynů vedoucího týmu • přebírá veškerou odpovědnost v případě nepřítomnosti vedoucího týmu • odpovídá za shromažďování a aktualizaci informací potřebných pro úspěšnou realizaci plánu
Systémové a aplikační zajištění *(roli může zastávat 1 až n zaměstnanců, jednotlivé odpovědnosti jsou pak rozděleny)*	• vykonává úkoly dle pokynů vedoucího týmu • odpovídá za celkový aktuální přehled instalací a konfigurací operačních systémů • odpovídá za celkový aktuální přehled instalací a konfigurací komunikačních prvků • udržuje aktuální přehled všech HW produktů, jejich konfigurace, nastavení, propojení apod. • udržuje aktuální přehled všech aplikačních produktů, jejich konfigurace, nastavení, propojení apod. • odpovídá za instalace konkrétních aplikačních produktů • udržuje přehled o stavu a aktuálnosti instalačních médií, návodů na instalace • udržuje přehled o stavu a aktuálnosti záloh dat
Člen týmu (*dle rozsahu havárie jsou do týmu jmenováni další zaměstnanci společnosti)*	• vykonává úkoly dle pokynů vedoucího týmu
Přizvaný člen týmu *(pro otestování funkčnosti obnoveného systému mohou být přizváni vhodní uživatelé)*	• vykonává úkoly dle pokynů vedoucího týmu • odpovídá za otestování funkčnosti obnoveného systému z uživatelského hlediska

4 PŘÍPRAVA PLÁNŮ

Rozsah a náplň plánu je vymezen *Šablonou plánu kontinuity a obnovy ICT* (kapitola 7).

- konkrétní požadavky pro její naplnění jsou uvedeny přímo v šabloně (*texty nápovědy jsou v šabloně psány kurzívou a jsou podbarveny, při zpracování plánů se nahradí požadovanými údaji, nejsou tak součástí finálního plánu)*
- zásady jako celek vymezují postup a doporučení pro zpracování plánu (naplnění šablony požadovanými údaji), jeho údržbu, testování a aktualizaci
- pro každý systém identifikovaný v rámci BIA jako klíčový musí být vytvořen samostatný plán kontinuity a obnovy (havarijní plán systému) plány obnovy klíčových systémů musí obsahovat detailní postupy jejich obnovy, vytvořené v souladu se šablonou plánů (kapitola 7) plány pro podpůrné systémy mohou být pouze rámcové – obsahují základní údaje (seznam HW, kontakty na dodavatele, apod.) potřebné pro zajištění obnovy
- navržené postupy pro zajištění kontinuity a obnovy IT služeb a podpůrných aktiv jsou vypracovávány v souladu se strategií[1] schválenou vedením společnosti.

Při přípravě plánů kontinuity a obnovy jednotlivých systémů jsou použity výstupy z provedené analýzy dopadů (*Business Impact Analysis, BIA*). Předmětem BIA je stanovit požadované časy (parametr RTO) a úroveň obnovy funkčnosti (parametr LBC) jednotlivých systémů. Zejména tyto údaje (tzv. parametry BCM) jsou hlavními vstupy pro stanovení odpovídajících strategií obnovy a vypracování havarijních plánů.

5 TESTOVÁNÍ A ÚDRŽBA PLÁNŮ

Vytvořené plány jsou předmětem pravidelných revizí, testování a aktualizací.

5.1 Testování plánů

Plány obnovy funkčnosti musí být pravidelně testovány.

Testování plánů je nezbytné a slouží k ověření použitelnosti v měnících se podmínkách. Testy by měly zejména určit místa havarijních plánu, která vyžadují modifikaci nebo aktualizaci, prověřit a procvičit znalosti a schopnosti jednotlivých členů týmu. Procvičování zajistí, že se odhalí různé nesrovnalosti a opomenutí v plánu dřív, než je použit ve skutečnosti. Testování plánů je nedílnou součástí preventivních opatření.

- rozsah testů musí být naplánován tak, aby byly v rámci 1 kalendářního roku postupně pokryty všechny náležitosti plánu (1 velký test nebo více malých)
- součástí testů musí být také ověření připravenosti záložních prostor
- testy musí probíhat tak, aby testovací procedury nenarušily normální chod systému
- je doporučeno, aby byly testy prováděny na náhradních prostředcích vlastních nebo prostředcích poskytnutých dodavatelem.

5.1.1 Harmonogram testování

Podle připraveného harmonogramu a scénářů se provádí testování dílčích částí a plánu jako celku.

[1] Strategie obnovy a vypracování havarijních plánů je jedním z výstupů procesu implementace BCM

- formulář pro přípravu scénářů je součástí šablony plánu (kapitola 7)
- scénář testování specifikuje požadavky na lidské a technické zdroje a obsahuje přesný harmonogram průběhu testu, včetně dne a času zahájení testu
- scénáře testování se připravují na základě výsledků a zkušeností z předchozích testů a na rozsahu relevantních změn, které v průběhu doby ve společnosti nastaly
- sestavení harmonogramu testování plánů je v kompetenci *Vedoucího havarijního týmu*, ten také odpovídá za průběh testování

5.1.2 Typy testů

Při testování plánů musí být postupováno od jednodušších testů ke složitějším.

Před prvním testováním se ověřuje srozumitelnost a logika plánu nezúčastněnou, ale znalou osobou.

Jednotlivé úrovně testů v podmínkách společnosti jsou:

- kontrola úplnosti plánů - nejjednodušší typ testů, který zahrnuje teoretické přezkoumání kompletnosti informací obsažených v plánech (provádí se např. ověření správnosti, úplnosti a aktuálnosti kontaktních údajů, seznamů technických prostředků, apod.)
- teoretický průchod plánem – tento typ testu je zaměřený na teoretické ověření proveditelnosti jednotlivých činností a postupů popsaných v plánech (např. časovou náročnost jednotlivých kroků, zda na sebe jednotlivé kroky logicky navazují, jestli jsou jednotlivé činnosti stručně, ale zároveň srozumitelně popsány, atd.)
- simulační testy - praktické nacvičování a prověření jednotlivých postupů a týmové interakce podle předem připravených scénářů (součástí testů je prověření funkčnosti komunikačních linek, otestování komunikace s dodavateli, zákazníky, médii a záchrannými složkami)
- paralelní testy - použití k tomu připravených, dle potřeby aktualizovaných kopií, replik a záloh z jednoho nebo více vybraných systémů v záložní lokalitě a jejich kompletní obnova na připraveném HW/SW v požadovaném čase. K tomu aby nebyl narušen běh paralelně a nepřetržitě běžících identických provozních systémů v primární lokalitě je u testů tohoto typu většinou nutné testovat v dočasně nebo trvale odděleném síťovém prostoru. (tyto testy jsou technicky zaměřené a jejich hlavním cílem je ověření schopnosti společnosti obnovit vybraný provozní systém v náhradní lokalitě a ověřit tím i možnost pokračovat v jeho provozu v případě vzniku mimořádné události na primární lokalitě).

5.1.3 Průběh testování

V průběhu testování musí být použity pouze zdroje, které budou použity v případě skutečné havárie.

- průběh testování musí být detailně zaznamenán (provádí vedoucí havarijního týmu nebo jím pověřený člen týmu.)
- záznam o průběhu a výsledcích testování plánu se provádí do formuláře uvedeného v šabloně (kapitola 7)

- v roli pozorovatele se testů účastní *Manažer bezpečnosti informací* nebo jím pověřená osoba[2]
- k testování mohou být také přizváni zástupci interního auditu, kteří zajistí zpětnou vazbu o průběhu testu, včetně srovnání výsledku testování s postupy popsanými v plánech
- na závěr testů musí být provedeno vyhodnocení (např. formou workshopu), na kterém se zhodnotí průběh a výsledky testování - je vhodné takovéto přezkoumání provádět přímo s účastníky, aby mohli vyjádřit svůj vlastní pohled a názor na průběh testu
- po provedeném testu musí být vypracována doporučení (např. formou stručné zprávy) na úpravy a zlepšení plánu
- veškeré nesrovnalosti a slabiny plánu, odhalené během testování, musí být co nejdříve zapracovány a publikována aktualizovaná verze plánu.

5.2 Údržba plánů

Plány musí vždy postihovat aktuální změny v systému (zejména pak na základě provedeného hodnocení rizik a analýzy dopadů), to je úkolem pravidelných revizí a aktualizací plánu.

- revize a aktualizace plánů musí být provedena nejen po každém testování, ale i při každé významnější změně, která může zásadně ovlivnit havarijní postupy
- nejméně jednou za 6 měsíců musí být provedena revize kontaktních informací (telefonní seznamy, kontakty na dodavatele, servisní služby, atd.)
- za pravidelnou revizi a aktualizaci plánů je odpovědný *Vedoucí havarijního týmu*
- všichni členové týmu pak odpovídají za zanesení aktuálních změn v rámci jim přidělených odpovědností
- po každé zásadní aktualizaci plánu zajistí *Vedoucí havarijního týmu* řízenou distribuci nové verze plánu a to výměnou za jeho předchozí verzi
- každá verze plánu musí být očíslována.

Je nutné, v odpovídajícím rozsahu, informovat klíčového uživatele systémů nebo aplikací začleněných do plánu obnovy daného systému o jakýchkoliv změnách v plánech, které ovlivňují způsob, jakým bude dosaženo kontinuity činností.

6 AKTIVACE PLÁNŮ

Každý zaměstnanec ČEPS musí neprodleně hlásit jakékoliv podezření na možnou bezpečnostní událost (incident nebo mimořádná událost, havárie), viz SM/88 Příloha č. 2.

Postupy hlášení bezpečnostních incidentů s dopadem na nutnost použití havarijních plánů musí být v souladu s příslušnou řídící dokumentací společnosti (SM/88 Příloha č. 8).

Vedoucí havarijního týmu (postiženého systému) po zhodnocení závažnosti rozhodne, zda se jedná o běžný bezpečnostní incident, který bude řešen postupy provozní operativy dle příslušných provozních postupů a pokynů, nebo se jedná o havárii.

[2] Cílem není pouze sledovat průběh testování a práce jednotlivých osob, ale nezávisle poskytnout zpětnou vazbu na průběh testování a napomoci ke zlepšení plánů.

V případě, že je situace havarijním týmem vyhodnocena jako mimořádná událost, jsou svoláni členové týmu a aktivován havarijní plán. Následující seznam událostí může vést k vyhlášení havarijního stavu a aktivaci havarijního plánu:

- úplné nebo částečné zničení technického zařízení
- zničení datového centra (voda, oheň, bomba, apod.)
- nedostupnost datového centra (anonymní výhružky, vyklizení budovy).

Pro každý z těchto dopadů je v plánu vypracován podrobný scénář, který popisuje jednotlivé kroky a činnosti členů havarijního týmu vedoucí k obnově funkčnosti systému. Smyslem scénářů je dopředu zvážit a logicky seřadit jednotlivé kroky, včetně odhadu jejich časové náročnosti. V rámci testování jsou scénáře zpřesňovány.

7 ŠABLONA PLÁNU KONTINUITY A OBNOVY ICT

POZNÁMKA: Texty podbarvené hnědě obsahují návod pro vyplnění. Při zpracování plánu se nahradí konkrétními údaji.

--- PRVNÍ STRANA PLÁNU ----

P L Á N K O N T I N U I T Y A O B N O V Y I C T
Uvede se název informačního systému
Identifikace pracoviště/datového centra (DC), kde se předpokládá nasazení plánu
Zpracoval:
Platnost:

--- DRUHÁ STRANA PLÁNU ---

Přehled o pravidelných revizích plánu

Jakékoliv aktualizace a změny provedené v tomto plánu musí být autorem zaznamenány v následující tabulce.

Datum	Verze	Popis změn	Změnil	Schválil
11/01/2010	1.0	Návrh první verze dokumentu		

Rozdělovník plánu

Rozdělovník obsahuje seznam zaměstnanců, kteří obdrží tištěnou nebo elektronickou podobu plánu.

Jméno	Kopie (Papírová/Elektronická)	Datum	Verze
	P/E		1.0
	E		
	P		

--- TĚLO PLÁNU ---

Rozsah plánu a scénáře

Tato část plánu je zaměřena na možné hrozby a jejich dopady. Následující seznam událostí může vést k vyhlášení havarijního stavu a aktivaci tohoto plánu:

- *Úplné nebo částečné zničení technického zařízení.*
- *Zničení datového centra (voda, oheň, bomba, apod.).*
- *Nedostupnost datového centra (anonymní výhružky, vyklizení budovy).*

Pro každý ze scénářů jsou zpracovány postupy obnovy systému, které podrobně popisují činnosti od vzniku mimořádné události po obnovení funkčnosti systému na požadovanou úroveň.

Hrozba	Možný dopad	Scénář: (protiopatření, k zajištění produktivity)	Číslo scénáře
Zničení DC[3] (voda, oheň, bomba)	**D1- D5**	Převedení provozu IS do alternativní (záložní) lokality	**1**
Totální tech. selhání HW	**D2, D5**	Obnovení provozu IS v ZDC	**2**
Technická závada HW / úmyslné poškození HW	**D2, D5**	Výměna zařízení (vlastní záložní nebo od dodavatele)	**2**
Selhání paměť. zařízení / chyba uživatele	**D3, D5**	Obnova dat ze záložních médií	**2**
Nedostupnost DC (anonymní výhružky, vyklizení budovy)	**D2- D5**	Vzdálený provoz a podpora informačních systémů	**3**

Poznámka: D1 - zničení HW, SW; D2 - přerušení fungování IS; D3 - ztráta kritických dat; D4 - chybné fungování IS; D5 - nedostupnost služby IS.

Scénář 1 - Převedení provozu IS do záložní lokality

Scénář pokrývá nejhorší variantu, kdy bude nutná kompletní/částečná obnova HW a infrastruktury v záložním datovém centru (DC). Tento scénář je realizován v případech, kdy bylo havarijním týmem rozhodnuto, z důvodu rozsahu havárie/poškození primárního DC, o převedení provozu do záložní lokality.

V rámci testování i v průběhu ostrého nasazení plánu musí být veškeré činnosti obnovy detailně dokumentovány, aby mohly být zde uvedené postupy obnovy případně aktualizovány nebo upřesněny – provádí určený člen týmu.

V následující tabulce je pro ilustraci uveden příklad fiktivního scénáře, v plánu se pochopitelně nahradí reálnými kroky a činnostmi. Obdobným způsobem se vypracují postupy pro scénáře č. 2 a 3.

[3] Datové centrum

Číslo kroku	Popis	Doba trvání
1	***Např. Svolání krizového týmu IT***	***2h***
	Krizový tým se schází na předem určeném místě	
	Ihned po svém příchodu se členové informují o aktuálním stavu a postupují podle svých plánů, odpovědností a podle aktuálních pokynů vedoucího týmu	
	V souladu se zásadami BOZP se přítomní členové havarijního týmu pokusí na místě havárie o záchranu záložních médií, neporušených IT prostředků, důležitých dokumentů, apod.	
	.....	
2	***Např. Zahájení přípravy záložního prostoru***	***5h***
	Vyzvednutí a doručení záložních kopií dat do záložní lokality – zajistí	
	Přesun odpovědných osob do záložní lokality – pracovníci odboru IT, a další členové týmu	
	Iniciace jednání s dodavateli záložního technického vybavení – zástupce vedoucí havarijního týmu	
	.....	
3	***Např. Instalace a konfigurace serverů, aplikací, síťových prvků .....***	***10h***
	Instalace operačních systémů na UNIX/Windows servery *Poznámka: v serverově záložní lokality jsou trvale umístěny servery s předinstalovanými operačními systémy*	
	Obnovení a File Server a File System na diskovém poli ze záloh	
	Obnova databáze ORACLE a prověření konzistence obnovených dat *POZNÁMKA: obnova může běžet paralelně s obnovou File System*	
	Instalace a zprovoznění všech aplikací dle stanoveného rozsahu, viz seznamy SW	
	Otestování funkčnosti instalací aplikací – určený člen týmu / vlastník aplikace	
	Konfigurace LAN a WAN	
	.....	
4	***Např. Otestování funkčnosti obnovených systémů***	***3h***
	Provedení funkčních testů uživateli	
	Provedení bezpečnostních testů (přístupových práv, apod.)	
	.....	
5	***Např. Zahájení ostrého provozu v záložní lokalitě***	***3h***
	Informování vedení společnosti o obnovení dostupnosti aplikací v záložní lokalitě	
	Informování dotčených pracovníků/uživatelů, aby se dostavili do záložní lokality.	
	.....	
	Konec (suma)	***58h (max. 60 hod)***

Scénář 2 - Obnovení provozu IS v DC

Scénář pokrývá nejhorší variantu, kdy bude nutná kompletní obnova HW a infrastruktury v primární datovém centru (DC), zároveň je také platný pro případ výměny konkrétních zařízení (v případě jejich závady/zničení) a pro případ obnovy dat ze záloh.

Tento scénář je realizován také v těch případech, kdy bylo krizovým týmem rozhodnuto, z důvodu rozsahu havárie/poškození DC, o dočasném zajištění dostupnosti systémů ČEPS v záložní lokalitě. Po skončení rekonstrukce je provoz převeden zpět do DC.

Do celkové doby realizace jednotlivých kroků tohoto scénáře není započtena doby rekonstrukce prostor datového centra. V závislosti na rozsahu škod může rekonstrukce probíhat v řádů týdnů až měsíců, v mezidobí je zajištěn provoz systému ze záložního pracoviště.

V rámci testování i v průběhu ostrého nasazení plánu musí být veškeré činnosti obnovy detailně dokumentovány, aby mohly být zde uvedené postupy obnovy případně aktualizovány nebo upřesněny – provádí určený člen týmu.

Číslo kroku	Popis	Doba trvání
1	***Např. Svolání havarijního týmu*** *Poznámka: tento krok je shodný se scénářem č.1*	**2h**
	Havarijní tým se schází na předem určeném místě *POZNÁMKA: V závislosti na rozsahu havárie je to přímo v primární lokalitě a nebo v předem vytipované budově v jejím okolí*	
	Ihned po svém příchodu se členové informují o aktuálním stavu a postupují podle svých plánů, odpovědností a podle aktuálních pokynů vedoucího týmu	
	V souladu se zásadami BOZP se přítomní členové krizového týmu pokusí na místě havárie o záchranu záložních médií, neporušených IT prostředků, důležitých dokumentů *POZNÁMKA: Pro dokumentaci stavu havárie, škod, prací a činností na místě havárie se v případě potřeby (např. pro pojišťovnu) používají další dokumentační prostředky, jako je fotografování a filmování).*	
	Rozhodnutí o obnovení provozu v DC nebo jeho převedení do záložní lokality a zahájení rekonstrukce v DC *POZNÁMKA: o přesunu provozu do záložní lokality bude zpravidla rozhodnuto v případech kdy dle prvního odhadu škod bude doba rekonstrukce odhadnuta na déle než 1 týden. V ostatních případech je přikročeno k zajištění obnovy přímo v primárním DC– další kroky scénáře jsou pro obě eventuality totožné.* *Obnova v původní lokalitě je zpravidla zahájena paralelně s kroky zajišťujícími dočasný provoz v záložní lokalitě. Dle rozsahu škod může obnova trvat týdny až měsíce.*	
	Iniciace jednání s dodavateli technického vybavení potřebných pro plnou obnovu systémů v DC (ověření a domluva dodacích lhůt, atd.)	
2	***Např. Dokončení přípravy původní lokality DC*** *POZNÁMKA: tento krok je zahájen poté co je ukončena rekonstrukce prostor DC a dodavateli zavezeno veškeré HW vybavení*	**10h**
	Zajistit zejména: • *zprovoznění komunikačních linek;* • *provedení instalace a konfigurace síťových prostředků;* • *pokud je to možné, reaktivovat požární a ostatní alarmy (alarmy proti vodě, alarmy průniku, atd.)* • *nepřetržitou ostrahu prostor, ve kterých se nachází důležitá aktiva;*	
3	***Např. Vytvoření aktuálních datových záloh***	**10h**
	Ukončení provozu v záložní lokalitě	
	Vytvoření aktuálních datových záloh provozovaných systémů v záložní lokalitě	
	Vyzvednutí a doručení záloh do primárního DC– členové havarijního týmu	
	Přesun odpovědných členů havarijního týmu do primárního DC	

4	***Např. Instalace operačních systémů na Windows servery, aplikací, síťových prvků***	**16h**
	Provést instalace operačních systémů ze standardních instalačních médií dle dokumentace dodavatelů a dle předem nacvičeného scénáře	
	Obnovení File Server a File System ze záloh	
	Obnova databáze MS SQLa prověření konzistence obnovených dat *POZNÁMKA: obnova může běžet paralelně s obnovou File System*	
	Instalace a zprovoznění všech aplikací	
	Otestování funkčnosti instalací aplikací – přizvaní uživatelé	
	Konfigurace LAN/WAN	
5	***Např. Konfigurace a instalace UNIX serveru***	**24h**
	Konfigurace UNIX serverů ve spolupráci s dodavatelem (cca 4hod)	
	Obnova databáze z aktuálních záloh a prověření konzistence obnovených dat (cca 7hod) *POZNÁMKA: nejprve musím být instalován SW pro obnovu dat ze záloh a připravena pásková knihovna.*	
	Ověření konektivity aplikací na databázi	
6	***Např. Otestování funkčnosti obnovených systémů***	**5h**
	Provedení funkčních testů uživateli	
	Provést bezpečnostní testy (přístupových práv, apod.)	
7	***Např. Zahájení ostrého provozu v primárním DC***	**5h**
	Informování vedení společnosti o obnovení dostupnosti systému v primárním DC	
	Informování všech pracovníků o obnovení dostupnosti systémů	
	Konec (suma)	

Scénář 3 - Vzdálený provoz a podpora informačních systémů

Tento scénář bude použit například v případě, že policie nechá vyklidit budovu ČEPS na základě anonymní zprávy o uložení bomby v budově.

V případě nedostupnosti prostor odkud je za normálních okolností prováděna správa a podpora systémů a aplikací se provádí činnosti v souladu s tímto scénářem.

V rámci testování i v průběhu ostrého nasazení plánu musí být veškeré činnosti obnovy detailně dokumentovány, aby mohly být zde uvedené postupy obnovy případně aktualizovány nebo upřesněny – provádí určený člen týmu.

Číslo kroku	Popis	Doba trvání
1	***Např. Vyhlášení krizové situace a evakuace budovy Bohdalec***	**2h**
	Určení zaměstnanci – členové havarijního týmu se přesunou do záložního pracoviště *Poznámka: O konkrétním rozdělení zaměstnanců v dané situaci rozhodne Vedoucí havarijního týmu*	
2	***Např. Vzdálená správa systémů***	**Po dobu evakuace**

	S pomocí autentizačního tokenu se pracovníci vzdáleně připojí do VPN a vykonávají činnosti spojené se správou systémů až do ukončení krizové situace	
3	***Např. Ukončení krizové situace***	**1h**
	Zaměstnanci se přesunou zpět do budovy na Bohdalci	

Kontaktní informace

Následující seznamy obsahují důležitá spojení, která mohou být v případě havárie použita. Jedná se o spojení na vedení ČEPS, členy havarijního týmu, záchrannou zdravotní službu, IT servisní firmy (HW, SW, komunikace, dodavatele aplikací, atd.), jiné servisní firmy z okolí (zámečníci, instalatéři, elektrikáři, atd.).

Havarijní tým

Zaznamenejte datum a čas kdy byli jednotliví členové týmu kontaktováni nebo byl uskutečněn pokus o jejich kontaktování v souvislosti s havarijní situací. Zaznamenejte, s jakým výsledkem byli jednotliví členové kontaktováni (zaneprázdněn, nedostupný, apod.).

KONTAKTNÍ ÚDAJE NA ČLENY HAVARIJNÍHO TÝMU			
Vedoucí týmu	Adresa	Tel:	Mobil (24hodin)
Kontaktoval	Datum/čas	Výsledek kontaktu	Poznámka
Zástupce vedoucího týmu	Adresa	Tel:	Mobil (24hodin)
Kontaktoval	Datum/čas	Výsledek kontaktu	Poznámka
Specialita sítě	Adresa	Tel:	Mobil (24hodin)
Kontaktoval	Datum/čas	Výsledek kontaktu	Poznámka

Systémové a aplikační zajištění	Adresa	Tel:	Mobil (24hodin)
Kontaktoval	Datum/čas	Výsledek kontaktu	Poznámka
Specialista SAN	Adresa	Tel:	Mobil (24hodin)
Kontaktoval	Datum/čas	Výsledek kontaktu	Poznámka
Člen týmu	Adresa	Tel:	Mobil (24hodin)
Kontaktoval	Datum/čas	Výsledek kontaktu	Poznámka
Člen týmu	Adresa	Tel:	Mobil (24hodin)
Kontaktoval	Datum/čas	Výsledek kontaktu	Poznámka

Kontakt na odpovědné osoby

Kontakt na osoby v rámci společnosti, které mohou být s ohledem na rozsah havarijní situace kontaktovány.

KONTAKTNÍ OSOBY V RÁMCI ČEPS				
Vedení ČEPS	**Jméno**	**Telefon**	**Mobil. tel.**	**e-mail**

Další kontaktní osoby				

Čísla tísňového volání

ČÍSLA TÍSŇOVÉHO VOLÁNÍ		
Složka	**Havarijní**	**Další spojení**
Hasiči	150	
Policie	158	
Lékařská pohotovost	155	
IZS	112	

Kontakt na externí firmy

Kontakt na IT servisní firmy, dodavatele aplikací, údržbářské a instalatérské firmy, apod. Musí být uvedena osoba (členy týmu) odpovědná za kontaktování dodavatele. Rychlost reakce dodavatele musí být započtena do celkového času obnovy systému.

KONTAKTY NA EXTERNÍ FIRMY					
Název firmy	**Oblast podpory**	**Adresa /tel./email**	**Kontaktní osoba**	**SLA: Doba reakce (čas v hod.)**	**Kontakt za ČEPS**

Místo setkání havarijního týmu

V okamžiku, kdy je nastalá událost posouzena jako havarijní, dochází ke svolání členů havarijního týmu.

Tým se schází v některé z předem vytipovaných místností (např. přímo v datovém centru nebo jeho bezprostřední blízkosti) tak, aby mohl být posouzen rozsah havárie přímo na místě a zahájeny kroky obnovy. V případě, že je událostí postižena celá budova pak se tým schází v některé z předem vytipovaných budov v okolí (náhradní místo setkání).

Vedoucím havarijního týmu nebo jeho zástupcem musí být předem prověřena připravenost místa setkání krizového týmu a zajištěna jeho přístupnost v potřebných časech.

V případě, že majitelem prostor je jiný subjekt než ČEPS, musí být přístup do vybraných prostor zajištěn smluvně.

PRIMÁRNÍ MÍSTO SETKÁNÍ TÝMU	
Objekt (budova):	
Ulice:	**Patro:**
Město/PSČ:	
Kontaktní osoba I:	**Tel:** **Mobil** **Fax:** **Další čísla:**
Kontaktní osoba II:	**Tel:** **Mobil:** **Fax:** **Další čísla:**
Poznámka:	

NÁHRADNÍ MÍSTO SETKÁNÍ TÝMU	
Objekt (budova):	
Ulice:	**Patro:**
Město/PSČ:	
Kontaktní osoba I:	**Tel:** **Mobil:** **Fax:** **Další čísla:**
Kontaktní osoba II:	**Tel:** **Mobil:** **Fax:** **Další čísla:**
Poznámka:	

DRUHÉ NÁHRADNÍ MÍSTO SETKÁNÍ TÝMU	
Objekt (budova):	
Ulice:	**Patro:**
Město/PSČ:	
Kontaktní osoba I:	**Tel:** **Mobil:** **Fax:** **Další čísla:**
Kontaktní osoba II:	**Tel:** **Mobil:** **Fax:** **Další čísla:**
Poznámka:	

Záložní lokalita obnovy

V případě, kdy rozsah havárie neumožňuje vytvoření záložních prostor přímo v budově, bude činnost přesunuta do záložních prostor v některé z níže uvedených lokalit. Vytipované záložní prostory musí mít předem zajištěnu odpovídající infrastrukturu (síťové přípojky, telefonní linky, apod.).

V případě, že majitelem záložních prostor je jiný subjekt než ČEPS, musí být přístup do vybraných prostor zajištěn smluvně.

ALTERNATIVNÍ LOKALITA	
Objekt (budova):	
Ulice:	**Patro:**
Město/PSČ:	
Kontaktní osoba I:	**Tel:** **Mobil:** **Fax:** **Další čísla:**
Kontaktní osoba II:	**Tel:** **Mobil:** **Fax:** **Další čísla:**

Poznámka:

Seznamy a schémata

Pokud existují jiné autoritativní seznamy je možné je do plánu zkopírovat, popř. se na ně odkázat.

Seznam softwaru

Uvede se přehled požadovaného SW, včetně umístění záložních kopií a odhadovaných časů obnovy. Kopie SW vytvářené pro účely záloh netvoří dodatečné náklady na licence.

Seznam softwaru						
Název programu	**OS**	**Počet ks. (médium)**	**Evid. č.**	**Umístění**	**Doba pro obnovu**	**Servisní firma**

Umístění záložních medií

Přehled a umístění datových záloh. Do poznámky je např. vhodné uvést osobu odpovědnou za vyzvednutí záloh a jejich dopravení do místa obnovy.

Umístění záložních médií						
IS/Aplikace	**Typ média**	**Počet ks.**	**Označení**	**Umístění**	**Doba pro obnovu**	**Další informace**

Seznam technického zařízení

Musí být uveden kompletní výčet zařízení potřebného pro funkčnost / obnovu systému.

Seznam technického zařízení (P – produkční, Z – záložní)					
Název zařízení	**P/Z**	**Evid. č.**	**Umístění**	**Doba pro obnovu**	**Servisní firma**

Uživatelské manuály a dokumentace

Musí být uveden i seznam všech důležitých dokumentů a zdrojů potřebných pro kontinuitu a obnovu systému. Plán musí také obsahovat podrobnosti o tom, kde jsou tyto dokumenty a zdroje umístěny. Dokumenty mohou obsahovat např. záznamy o tom, kdo je pověřen získat hesla, kterých bude zapotřebí.

Dokumentace pro obnovu informačních systémů		
Popis	**Umístění**	**Další informace**

Seznam dostupných technických prostředků

Pro případ, kdy je požadována foto, nebo filmová dokumentace (např. za účelem zmapování rozsahu škod pro pojišťovnu) musí být uveden seznam dostupných prostředků spolu s jejich umístěním a dispozicemi. Musí být určena osoba odpovědná za technický stav těchto prostředků (baterie, funkčnost, atd.). Potřebné materiály mohou také zahrnovat kancelářské potřeby, náhradní díly, speciální strojní zařízení a nástroje.

Prostředek	**Umístění**	**Odpovědná osoba/Kontakt**
Např. Fotoaparát		
Např. Kamera		
Např. Svítilny		

Např. Dopravní prostředky		

Záznamy o rozhodnutích a činnostech týmu

Záznamy provádí Vedoucí havarijního týmu, případně člen týmu, který je jako první přítomen na pracovišti v průběhu havárie.

Záznamy by měly být co nejpodrobnější, aby mohl být následně zmapován celý průběh zvládání havárie a případně přijata nápravná opatření.

Jakékoliv alternativní postupy učiněné v rámci havárie, odlišné od postupů popsaných v plánu, musí být zaznamenány a následně musí být vhodným způsobem provedena aktualizace plánu.

ZÁZNAMY O ROZHODNUTÍCH A ČINNOSTECH TÝMU			
Datum:		**Čas:**	
Jméno:		**Podpis:**	
Činnost	**Komentář**		

Záznamy o pravidelném testování plánu

V rámci testování i v průběhu ostrého nasazení plánu musí být veškeré činnosti obnovy detailně dokumentovány, aby mohly být zde uvedené postupy obnovy případně aktualizovány nebo upřesněny – provádí zástupce vedoucího, popř. jiný určený člen havarijního týmu.

SCÉNÁŘ TESTOVÁNÍ	
Název IS / aplikace:	
Verze plánu:	**Typ testu:**
Schválení scénáře testování	
Správce IS / aplikace:	
Kontakt: (telefon,e-mail)	**Podpis:**
Zpracovatel havarijního plánu:	
Kontakt: (telefon,e-mail)	
Schválil:	
Kontakt: (telefon,e-mail)	**Podpis:**
Datum a čas zahájení testu:	
Odhad délky trvání testu (hod):	
SCÉNÁŘ TESTOVÁNÍ HAVARIJNÍHO PLÁNU	
Jaká havárie bude simulována:	
(havárie, která může v provozu nastat a pro kterou se bude plán testovat)	
Co bude testováno:	
(popsat co (přesně) bude simulováním havárie testováno)	
Postup testování:	
(popsat v jednotlivých krocích: číslo kroku, tým nebo ID úkolu, popis, plánovaný čas)	
Vliv testu na provoz dalších aplikací/IS:	

(uvést negativní dopady provádění testu na provoz(dostupnost) dalších aplikací)
Požadovaná součinnost útvarů IT: *(uvést jména útvarů/pracovníků a požadovanou součinnost)*
Požadovaná součinnost útvarů mimo IT: *(uvést jména útvarů/pracovníků a požadovanou součinnost)*
Další nutné podmínky umožňující provedení testu: *(možná omezení nebo podmínky pro provedení testu, apod.)*

Vyhodnocení průběhu testování

Výsledky testování musí být v co nejkratším termínu přezkoumány, aby mohly být plán aktualizován. Protokol z testování by měl obsahovat i názor nezávislých pozorovatelů.

VYHODNOCENÍ TESTOVÁNÍ	
Název IS / aplikace:	
Verze plánu:	**Typ testu:**
Schválení výsledků testování	
Výsledek testu: ***úspěšný / neúspěšný***	
Správce IS / aplikace:	
Kontakt: (telefon, e-mail)	**Podpis:**
Zpracovatel plánu:	
Kontakt: (telefon, e-mail)	
Schválil:	
Kontakt: (telefon, e-mail)	**Podpis:**
Datum a čas ukončení testu:	
Délka trvání testu (hod):	
Navrhovaná doba pro obnovu fungování IS (hod):	

VYHODNOCENÍ PROVEDENÉHO TESTU PLÁNU
Postup testování: *(číslo kroku, tým nebo ID úkolu, popis, splněno A/N, dosažený čas – na konci tabulky součet všech časů = délka trvání testu)*
Vyhodnocení jednotlivých týmů: *(tým, vedoucí týmu, splněno A/N)*
Vyhodnocení testu *(v případě neúspěšného testu analýza příčin neúspěchu)*
Doporučení změn v plánu: *(veškerá doporučení a možnosti pro zlepšení postupů obnovy, úrovně detailů uvedených v plánu, apod.)*