					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P32					Název dokumentu: **Politika kontinuity činností a obnovy po havárii**							
Verze: 1.0		Datum účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Standard		Postup		Formulář		Registr		Jiné	

Historie revizí				
Číslo revize	**Datum revize**	**Změny**	**Přezkoumal**	**Vlastník procesu**

Schválení			
Jméno	**Funkce**	**Datum**	**Podpis**

V souladu s normami a právními předpisy

Norma / právní předpis	Kapitola / článek	Komentář
ISO/IEC 27001:2022	Kapitola 8	
ISO/IEC 27002:2022	Opatření 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-1 až CP-11	
NIST SP 800-34 Rev.1	Plánování pro mimořádné situace	Rámec
ISO 22301:2019		Požadavky na systém managementu kontinuity činností
GDPR	Článek 32	
směrnice NIS2	Článek 21 odst. 2 písm. f)	
nařízení DORA	Článek 10	
COBIT 2019	DSS	

1. Účel

1.1. Tato politika stanoví závazná opatření a odpovědnosti k zajištění schopnosti organizace zachovat nebo obnovit kritické obchodní operace a podpůrné ICT služby během narušujícího incidentu a po něm.

1.2. Cílem je chránit životy, provozní stabilitu, plnění právních povinností, závazky vůči zákazníkům a pověst organizace prostřednictvím začlenění odolnosti na základě proaktivního plánování a ověřených schopností obnovy.

1.3. Tato politika vytváří základ rámce organizace pro řízení kontinuity činností (BCM) a obnovu po havárii (DR) a zajišťuje soulad s příslušnými regulačními, smluvními a oborovými požadavky.

2. Rozsah

2.1. Tato politika se vztahuje na všechny organizační útvary, informační systémy, podnikové procesy, pracovníky a služby třetích stran, které jsou na základě výsledků analýzy dopadů na činnost organizace (BIA) klasifikovány jako kritické nebo nezbytné.

2.2. Politika zahrnuje:

2.2.1. narušení přírodního i antropogenního původu, včetně kybernetických útoků, selhání infrastruktury, výpadků datových center, pandemií a přerušení služeb dodavatelů,

2.2.2. plánování, testování a průběžné zlepšování plánů kontinuity činností (BCP) a plánů obnovy po havárii (DRP),

2.2.3. role a odpovědnosti pro reakci na mimořádné situace, koordinaci obnovy a eskalaci incidentů.

2.3. Ustanovení této politiky jsou závazná pro všechny pracovníky s odpovědnostmi v oblasti kontinuity nebo obnovy, včetně IT, vlastníků procesů, krizových manažerů a dodavatelů.

3. Cíle

3.1. Zajistit kontinuitu provozu a služeb prostřednictvím předem definovaných a testovaných postupů a minimalizovat provozní, reputační a právní dopady.

3.2. Obnovit ICT služby ve stanovených cílových dobách obnovy (RTO) a cílových bodech obnovy (RPO) v souladu s úrovní tolerance obchodních rizik.

3.3. Jednoznačně přiřadit odpovědnost za plánování, realizaci a správu kontinuity činností a obnovy po havárii v celé organizaci.

3.4. Zajistit, aby schopnosti kontinuity byly pravidelně testovány, udržovány a zlepšovány na základě realistických scénářů a zjištění z auditů.

3.5. Plnit povinnosti v oblasti souladu podle ISO, NIST, GDPR, DORA a NIS2 a podporovat náležitou péči v oblasti provozní odolnosti a dostupnosti.

4. Role a odpovědnosti

4.1. Vrcholové vedení

4.1.1. Schvaluje Politiku kontinuity činností a obnovy po havárii a zajišťuje její strategické sladění.

4.1.2. Přiděluje rozpočet a zdroje na podporu kontinuity činností, reakce na mimořádné situace a cvičení obnovy.

4.2. Manažer kontinuity činností (vedoucí BCM)

4.2.1. Odpovídá za tvorbu a údržbu plánů kontinuity činností (BCP) na úrovni celé organizace a za koordinaci testování kontinuity.

4.2.2. Udržuje harmonogram BIA, zajišťuje školení a ověřuje, že dokumentace splňuje požadavky na soulad.

[... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ...]

9. Požadavky na přezkoumávání a aktualizaci

9.1. Tato politika musí být každoročně přezkoumána manažerem kontinuity činností a ředitelem informační bezpečnosti (CISO), aby bylo zajištěno její sladění s:

9.1.1. změnami v obchodních operacích, kritických systémech nebo infrastruktuře,

9.1.2. poznatky získanými z incidentů, auditů, stolních cvičení nebo testů DR,

9.1.3. aktualizovanými regulačními nebo smluvními povinnostmi (např. DORA, GDPR, požadavky zákazníků na RTO/RPO),

9.1.4. změnami v ochotě organizace podstupovat riziko nebo ve strategii kontinuity.

9.2. Přezkumy musí zahrnovat:

9.2.1. ověření relevance plánů a kontaktních údajů,

9.2.2. opětovné posouzení RTO, RPO a zařazení obnovy do úrovní,

9.2.3. vyhodnocení kapacity služeb zálohování a DR,

9.2.4. zpětnou vazbu od zainteresovaných stran, které realizovaly nedávné plány obnovy nebo testy.

9.3. Všechny změny politiky musí být:

9.3.1. vedeny v režimu správy verzí se zdokumentovaným odůvodněním a schválením zainteresovanými stranami,

9.3.2. oznámeny klíčovým pracovníkům a týmům s aktualizovanými odpovědnostmi,

9.3.3. promítnuty do aktualizovaných školení, materiálů pro zvyšování povědomí a provozních postupů.

9.4. Nouzové dočasné aktualizace musí být vydány v případě významné organizační změny, právního požadavku nebo kritického zjištění, v jehož důsledku stávající plány nebo tato politika již nejsou použitelné.

10. Související politiky a vazby

10.1. Tato politika se uplatňuje v koordinaci s následujícími klíčovými dokumenty:

10.1.1. P1 – Politika informační bezpečnosti: stanoví požadavek na provoz založený na rizicích a odolnosti za všech podmínek.

10.1.2. P5 – Politika řízení změn: zajišťuje, aby veškeré změny konfigurace nebo infrastruktury související s obnovou probíhaly podle zdokumentovaných a schválených pracovních postupů.

10.1.3. P14 – Politika uchovávání údajů: upravuje životní cyklus záložních médií a obnovených dat používaných při zajištění kontinuity.

10.1.4. P15 – Politika zálohování a obnovy: stanoví opatření týkající se frekvence zálohování, zabezpečení a ověřování obnovy.

10.1.5. P18 – Politika kryptografických opatření: zajišťuje, aby procesy obnovy dodržovaly standardy šifrování a důvěrnosti.

10.1.6. P22 – Politika protokolování a monitorování: podporuje detekci a eskalaci událostí s dopadem na kontinuitu.

10.1.7. P30 – Politika reakce na incidenty: definuje procesy zamezení šíření, eskalace a analýzy kořenové příčiny v souladu se spouštěči kontinuity.

10.1.8. P33 – Politika monitorování auditu a souladu: ověřuje integritu a účinnost postupů kontinuity a obnovy napříč systémy a procesy.

11. Referenční normy a rámce

11.1. Tato politika je v souladu s mezinárodně uznávanými normami pro kontinuitu činností a obnovu po havárii a podporuje auditovatelnost, odolnost a právní soulad.

11.2. ISO/IEC 27002

11.2.1. Příloha A, opatření 5.29 – Bezpečnost informací během narušení: vyžaduje kontinuitu bezpečnostních opatření za nepříznivých podmínek.

11.2.2. Příloha A, opatření 5.30 – Připravenost ICT na kontinuitu činností: stanoví povinnost přípravy, testování a validace schopností obnovy ICT.

11.3. ISO 22301:2019 – Systémy managementu kontinuity činností

11.3.1. Poskytuje rámec pro zavedení, implementaci a udržování postupů BCM v souladu s cíli organizace a prahovými hodnotami rizik.

11.4. NIST SP 800-34 Rev.1 – Příručka pro plánování mimořádných situací

11.4.1. Stanoví osvědčené postupy pro plány zvládání mimořádných situací v IT, včetně tvorby strategie kontinuity, analýzy dopadů a testování plánů.

11.5. GDPR (2016/679)

11.5.1. Článek 32 – Zabezpečení zpracování: vyžaduje odolnost systémů zpracování a včasnou obnovu dostupnosti a přístupu k osobním údajům po incidentu.

11.6. směrnice NIS2 (2022/2555)

11.6.1. Článek 21 odst. 2 písm. f): stanoví opatření v oblasti kontinuity činností a krizového řízení na podporu bezpečnosti sítí a informačních systémů.

11.7. nařízení DORA (2022/2554)

11.7.1. Článek 10 – Kontinuita činností ICT: vyžaduje, aby finanční subjekty vytvářely a testovaly plány kontinuity ICT, včetně RTO/RPO založených na riziku a schopností přepnutí na záložní prostředí.

11.8. COBIT 2019

11.8.1. DSS04 – Řízení kontinuity: pokrývá všechny aspekty plánování kontinuity, včetně identifikace hrozeb, analýzy dopadů, strategie obnovy a pravidelného testování.