					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P32S					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	Články 6.1, 6.3, 8	
ISO/IEC 27002:2022	Opatření 5.29, 5.30	
NIST SP 800-53 Rev. 5	CP-2, CP-4, CP-6, CP-7	
GDPR	Články 32, 33	
směrnice NIS2	Článek 21 odst. 2 písm. f)	
nařízení DORA	Článek 10	
COBIT 2019	DSS04	

1. Účel

1.1 Tato politika zajišťuje, aby organizace byla schopna zachovat provozní činnosti a obnovit nezbytné IT služby během narušujících událostí a po nich, jako jsou výpadky napájení, kybernetické útoky, ransomware nebo selhání systémů.

1.2 Stanovuje jasný rámec pro plánování kontinuity činností a obnovy po havárii (BC/DR), přizpůsobený potřebám SME bez vyčleněných IT týmů.

1.3 Tato politika pomáhá organizaci plnit závazné požadavky podle ISO/IEC 27001:2022, GDPR, NIS2, DORA a COBIT 2019 a současně posilovat provozní odolnost a důvěru zákazníků.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 všechny systémy a služby kritické pro podnikání (např. e-mail, cloudová úložiště, fakturační platformy, zákaznické záznamy),

2.1.2 všechny zaměstnance a externí poskytovatele IT služeb odpovědné za připravenost a realizaci BC/DR,

2.1.3 všechny typy narušení, včetně kybernetických incidentů, selhání hardwaru, výpadků napájení, záplav a nedostupnosti kanceláří.

2.2 Pokrývá zejména:

2.2.1 řízení zálohování,

2.2.2 plánování kontinuity činností (BCP),

2.2.3 činnosti obnovy po havárii,

2.2.4 školení personálu a testování,

2.2.5 právní a regulační postupy reakce.

3. Cíle

3.1 Chránit schopnost organizace poskytovat klíčové služby navzdory neplánovaným narušením.

3.2 Zajistit včasnou obnovu systémů a dat podle předem stanovených cílových dob obnovy (RTO).

3.3 Umožnit všem pracovníkům postupovat během krizových situací podle postupů kontinuity s minimem nejasností.

3.4 Udržovat soulad s právními požadavky na ochranu osobních údajů a provozní odolnost, včetně článku 32 GDPR a článku 21 směrnice NIS2.

3.5 Zavést praktickou a testovatelnou strategii kontinuity a obnovy vhodnou pro SME.

4. Role a odpovědnosti

4.1 generální ředitel (GM)

4.1.1 odpovídá za proces BC/DR a za tuto politiku,

4.1.2 schvaluje Plán kontinuity činností (BCP),

4.1.3 koordinuje reakci na incidenty a interní komunikaci během narušení,

4.1.4 zajišťuje regulatorní oznámení podle potřeby (např. oznámení porušení zabezpečení osobních údajů podle GDPR).

4.2 poskytovatel IT služeb / správce systému

4.2.1 udržuje a testuje zálohy,

4.2.2 provádí postupy obnovy po havárii při jejich aktivaci,

4.2.3 dokumentuje všechny kroky obnovy a události související s obnovou systémů,

4.2.4 neprodleně hlásí kritické IT incidenty generálnímu řediteli (GM).

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

9. Požadavky na přezkoumávání a aktualizaci

9.1 Každoroční přezkum politiky a plánu

9.1.1 Generální ředitel (GM) musí zajistit, aby tato politika a související Plán kontinuity činností (BCP) byly formálně přezkoumány alespoň jednou ročně.

9.1.2 Přezkum musí zahrnovat:

9.1.2.1 vyhodnocení nově vznikajících rizik,

9.1.2.2 opětovné potvrzení RTO/RPO,

9.1.2.3 ověření informací o dodavatelích a kontaktních údajů,

9.1.2.4 sladění se změnami v IT systémech, právních povinnostech nebo provozu.

9.2 Aktualizace na základě spouštěcích událostí

9.2.1 Tato politika musí být aktualizována také v reakci na:

9.2.1.1 významné incidenty nebo narušení, zejména pokud nebyly splněny cíle,

9.2.1.2 nové právní nebo regulační povinnosti (např. změny DORA),

9.2.1.3 změny v kritických systémech, cloudových platformách nebo personálu,

9.2.1.4 zjištění z každoročních testů BCP/DR.

9.3 Proces řízení změn

9.3.1 Všechny změny musí schválit GM.

9.3.2 Musí být vedena historie verzí včetně data, popisu změny a schvalovatele.

9.3.3 Aktualizovaná politika musí být znovu distribuována všem relevantním osobám, včetně poskytovatele IT služeb a vedoucích oddělení.

9.4 Dokumentace získaných poznatků

9.4.1 Po testech nebo skutečných narušeních musí být zdokumentované získané poznatky promítnuty do budoucích aktualizací.

9.4.2 Tyto přezkumy musí zahrnovat také hodnocení výkonnosti dodavatelů a ověření přiměřenosti reakce.

10. Související politiky a vazby

10.1 Tato politika je úzce propojena s následujícími politikami SME:

10.1.1 P1S – P01 Politika informační bezpečnosti: Vymezuje cíle bezpečnosti na vysoké úrovni, které musí postupy kontinuity a obnovy podporovat.

10.1.2 P4S – Politika řízení přístupu: Umožňuje nouzové odebrání nebo obnovení uživatelských přístupů během scénářů narušení činností.

10.1.3 P6S – Politika řízení rizik: Tvoří základ pro identifikaci, hodnocení a prioritizaci rizik souvisejících s kontinuitou.

10.1.4 P8S – Politika zvyšování povědomí o informační bezpečnosti a školení: Zajišťuje, aby zaměstnanci byli připraveni jednat během narušení a rozuměli BCP.

10.1.5 P15S – Politika zálohování a obnovy: Poskytuje konkrétní technické postupy pro zajištění dostupnosti dat a obnovy.

10.1.6 P17S – Politika ochrany dat a soukromí: Zajišťuje, aby plánování kontinuity respektovalo ochranu osobních údajů a bylo během incidentů i po nich v souladu s GDPR.

10.1.7 P22S – Politika protokolování a monitorování: Podporuje detekci událostí, které mohou aktivovat procesy BC/DR, a poskytuje forenzní auditní stopu po narušení.

10.1.8 P30S – Politika reakce na incidenty: Bezprostředně předchází aktivaci procesu obnovy v případě kybernetických nebo provozních incidentů.

10.1.9 P31S – Politika shromažďování důkazů a forenzní analýzy: Zajišťuje zachycení digitálních důkazů během scénářů kontinuity pro účely souladu, pojištění nebo vyšetřování.

10.2 Tyto politiky tvoří soudržný rámec připravený na audit pro odolnost, odpovědnost a kontinuitu kontrol napříč všemi činnostmi SME.

11. Referenční normy a rámce

11.1 ISO/IEC 27001:

11.1.1 Článek 6.1 – Vyžaduje plánování a ošetření rizik, včetně kontinuity činností a obnovy.

11.1.2 Článek 6.3 – Zdůrazňuje neustálé zlepšování po narušeních.

11.1.3 Článek 8.1 – Ukládá provozní opatření, která zahrnují i zdokumentovaná opatření kontinuity.

11.2 ISO/IEC 27002:

11.2.1 Opatření 5.29 – Vyžaduje zavedení a udržování opatření pro kontinuitu činností.

11.2.2 Opatření 5.30 – Vyžaduje testování a přezkum těchto opatření.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 CP-2 – Definuje požadavky na plánování mimořádných situací.

11.3.2 CP-4 – Ukládá školení personálu organizace pro mimořádné situace.

11.3.3 CP-6 – Pokrývá požadavky na alternativní místo uložení.

11.3.4 CP-7 – Stanoví požadavky na alternativní místo zpracování.

11.4 GDPR:

11.4.1 Článek 32 – Vyžaduje opatření k zajištění průběžné dostupnosti a odolnosti systémů a služeb zpracování.

11.4.2 Článek 33 – Aktivuje oznamovací povinnosti při porušení zabezpečení osobních údajů v případech, kdy selhání kontinuity vede ke kompromitaci osobních údajů.

11.5 směrnice NIS2 (2022/2555):

11.5.1 Článek 21 odst. 2 písm. f) – Vyžaduje plánování kontinuity a schopnosti krizového řízení jako podmínku připravenosti na kybernetická rizika.

11.6 nařízení DORA (2022/2554):

11.6.1 Článek 10 – Ukládá zavedení testování digitální provozní odolnosti a schopností obnovy, zejména pro SME ve finančním sektoru.

11.7 COBIT 2019:

11.7.1 DSS04 – Řízení kontinuity: Poskytuje pokyny pro správu a řízení podniku k udržování a ověřování provozní odolnosti, včetně vlastnictví, testování, zapojení dodavatelů a přezkumů po událostech.