					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P32					Názov dokumentu: **Politika kontinuity činností a obnovy po havárii**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Štandard		Postup		Formulár		Register		Iné	

História revízií				
Číslo revízie	**Dátum revízie**	**Zmeny**	**Preskúmal**	**Vlastník procesu**

Schválenia			
Meno	**Pozícia**	**Dátum**	**Podpis**

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitola 8	
ISO/IEC 27002:2022	Kontroly 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-1 až CP-11	
NIST SP 800-34 Rev.1	Plánovanie nepredvídaných udalostí	Rámec
ISO 22301:2019		Požiadavky na systém manažérstva kontinuity činností
Nariadenie EÚ GDPR	Článok 32	
Smernica EÚ NIS2	Článok 21(2)(f)	
Nariadenie EÚ DORA	Článok 10	
COBIT 2019	DSS	

1. Účel

1.1. Táto politika stanovuje záväzné kontroly a zodpovednosti na zabezpečenie schopnosti organizácie udržať alebo obnoviť kritické podnikové činnosti a podporné IKT služby počas narušujúceho incidentu a po jeho skončení.

1.2. Jej cieľom je chrániť život, prevádzkovú stabilitu, plnenie zákonných povinností, záväzky voči zákazníkom a reputáciu organizácie prostredníctvom začlenenia odolnosti do proaktívneho plánovania a validovaných schopností obnovy.

1.3. Táto politika poskytuje základ pre rámec organizácie v oblasti riadenia kontinuity činností a obnovy po havárii a zabezpečuje súlad s uplatniteľnými regulačnými, zmluvnými a odvetvovými požiadavkami.

2. Rozsah

2.1. Táto politika sa vzťahuje na všetky organizačné jednotky, informačné systémy, podnikové procesy, personál a služby tretích strán, ktoré sú na základe výsledkov analýzy vplyvu na podnikanie (BIA) klasifikované ako kritické alebo nevyhnutné.

2.2. Politika sa vzťahuje na:

2.2.1. Prírodné a človekom spôsobené narušenia vrátane kybernetických útokov, zlyhaní infraštruktúry, výpadkov dátových centier, pandémií a prerušení služieb dodávateľov

2.2.2. Plánovanie, testovanie a nepretržité zlepšovanie plánov kontinuity činností (BCP) a plánov obnovy po havárii (DRP)

2.2.3. Roly a zodpovednosti za reakciu na núdzové situácie, koordináciu obnovy a eskaláciu incidentov

2.3. Ustanoveniam tejto politiky podliehajú všetci zamestnanci s povinnosťami v oblasti kontinuity činností alebo obnovy vrátane IT, vlastníkov podnikových procesov, krízových manažérov a dodávateľov.

3. Ciele

3.1. Zabezpečiť kontinuitu podnikových činností a služieb prostredníctvom vopred definovaných a otestovaných postupov s cieľom minimalizovať prevádzkový, reputačný a právny dosah.

3.2. Obnoviť IKT služby v rámci definovaných cieľových časov obnovy (RTO) a cieľových bodov obnovy (RPO) v súlade s úrovňami tolerancie podnikových rizík.

3.3. Priradiť vlastníctvo plánovania, vykonávania a riadenia kontinuity činností a obnovy po havárii v rámci celej organizácie.

3.4. Zabezpečiť, aby boli schopnosti kontinuity pravidelne testované, udržiavané a zlepšované na základe realistických scenárov a auditných zistení.

3.5. Plniť povinnosti v oblasti súladu podľa ISO, NIST, GDPR, DORA a NIS2 a podporovať náležitú starostlivosť v oblasti prevádzkovej odolnosti a dostupnosti.

4. Roly a zodpovednosti

4.1. Vrcholové vedenie

4.1.1. Schvaľuje Politiku kontinuity činností a obnovy po havárii a zabezpečuje jej strategické zosúladenie.

4.1.2. Prideľuje rozpočet a zdroje na podporu kontinuity činností, reakcie na núdzové situácie a cvičení obnovy.

4.2. Manažér kontinuity činností (vedúci BCM)

4.2.1. Zodpovedá za vypracovanie a údržbu celopodnikových BCP a za koordináciu testovania kontinuity.

4.2.2. Udržiava harmonogram BIA, zabezpečuje školenia a zaisťuje, aby dokumentácia spĺňala požiadavky na súlad.

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Požiadavky na preskúmanie a aktualizáciu

9.1. Túto politiku musí každoročne preskúmať Manažér kontinuity činností a CISO, aby sa zabezpečilo zosúladenie s:

9.1.1. zmenami v podnikových činnostiach, kritických systémoch alebo infraštruktúre

9.1.2. poznatkami získanými z incidentov, auditov, cvičení pri stole alebo testov DR

9.1.3. aktualizovanými regulačnými alebo zmluvnými povinnosťami (napr. DORA, GDPR, požiadavky zákazníkov na RTO/RPO)

9.1.4. zmenami apetítu organizácie na riziko alebo stratégie kontinuity

9.2. Preskúmania musia zahŕňať:

9.2.1. validáciu relevantnosti plánov a kontaktných údajov

9.2.2. prehodnotenie RTO, RPO a úrovní obnovy

9.2.3. vyhodnotenie kapacity služieb zálohovania a DR

9.2.4. spätnú väzbu od zainteresovaných strán, ktoré realizovali nedávne plány obnovy alebo testy

9.3. Všetky zmeny politiky musia byť:

9.3.1. riadené verziami so zdokumentovaným odôvodnením a schválením zainteresovanými stranami

9.3.2. oznámené kľúčovým pracovníkom a tímom s aktualizovanými zodpovednosťami

9.3.3. premietnuté do aktualizovaných školení, materiálov na zvyšovanie povedomia a prevádzkových postupov

9.4. Núdzové priebežné aktualizácie musia byť vydané, ak dôjde k významnej organizačnej zmene, právnemu príkazu alebo kritickému zisteniu, v dôsledku ktorého aktuálne plány alebo politika už nie sú použiteľné.

10. Súvisiace politiky a väzby

10.1. Táto politika sa uplatňuje v koordinácii s týmito kľúčovými dokumentmi:

10.1.1. P1 – Politika informačnej bezpečnosti: Stanovuje požiadavku na prevádzku odolnú voči rizikám za všetkých okolností.

10.1.2. P5 – Politika riadenia zmien: Zabezpečuje, aby všetky zmeny konfigurácie alebo infraštruktúry súvisiace s obnovou prechádzali zdokumentovanými a schválenými postupmi.

10.1.3. P14 – Politika uchovávania a likvidácie údajov: Upravuje životný cyklus zálohovacích médií a obnovených údajov používaných pri činnostiach kontinuity.

10.1.4. P15 – Politika zálohovania a obnovy: Uplatňuje kontroly frekvencie zálohovania, bezpečnosti a overovania obnovy.

10.1.5. P18 – Politika kryptografických kontrol: Zabezpečuje, aby procesy obnovy zachovávali štandardy šifrovania a dôvernosti.

10.1.6. P22 – Politika logovania a monitorovania: Podporuje detekciu a eskaláciu udalostí ovplyvňujúcich kontinuitu.

10.1.7. P30 – Politika reakcie na incidenty: Definuje procesy zamedzenia šírenia, eskalácie a analýzy hlavnej príčiny zosúladené so spúšťačmi kontinuity.

10.1.8. P33 – Politika monitorovania auditu a súladu: Overuje integritu a účinnosť postupov kontinuity a obnovy naprieč systémami a procesmi.

11. Referenčné normy a rámce

11.1. Táto politika je zosúladená s medzinárodne uznávanými normami pre kontinuitu činností a obnovu po havárii a podporuje auditovateľnosť, odolnosť a právny súlad.

11.2. ISO/IEC 27002

11.2.1. Príloha A, kontrola 5.29 – informačná bezpečnosť počas narušenia: Vyžaduje kontinuitu bezpečnostných kontrol v nepriaznivých podmienkach.

11.2.2. Príloha A, kontrola 5.30 – pripravenosť IKT na kontinuitu činností: Vyžaduje prípravu, testovanie a validáciu schopností obnovy IKT.

11.3. ISO 22301:2019 – systémy manažérstva kontinuity činností

11.3.1. Poskytuje rámec na zavedenie, implementáciu a udržiavanie postupov BCM v súlade s cieľmi organizácie a prahovými hodnotami rizika.

11.4. NIST SP 800-34 Rev.1 – príručka plánovania nepredvídaných udalostí

11.4.1. Stanovuje osvedčené postupy pre plány nepredvídaných udalostí pre IT systémy vrátane vypracovania stratégie kontinuity, analýzy dosahov a testovania plánov.

11.5. Nariadenie EÚ GDPR (2016/679)

11.5.1. Článok 32 – bezpečnosť spracúvania: Vyžaduje odolnosť systémov spracúvania a včasnú obnovu dostupnosti a prístupu k osobným údajom po incidente.

11.6. Smernica EÚ NIS2 (2022/2555)

11.6.1. Článok 21(2)(f): Vyžaduje opatrenia v oblasti kontinuity činností a krízového riadenia na podporu bezpečnosti sietí a informačných systémov.

11.7. Nariadenie EÚ DORA (2022/2554)

11.7.1. Článok 10 – kontinuita činností IKT: Vyžaduje, aby finančné subjekty vypracovali a testovali plány kontinuity IKT vrátane RTO/RPO založených na riziku a schopností prepnutia na záložné prostredie.

11.8. COBIT 2019

11.8.1. DSS04 – riadenie kontinuity: Zahŕňa všetky aspekty plánovania kontinuity vrátane identifikácie hrozieb, analýzy dosahov, stratégie obnovy a pravidelného testovania.