					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P15					Názov dokumentu: **Politika zálohovania a obnovy**							
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**

Zosúladenie s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitoly 6.1.3, 8.	Ošetrenie rizík, plánovanie a prevádzkové kontroly zálohovania
ISO/IEC 27002:2022	Kontroly 8.13, 5.28, 5.	Riadenie zálohovania, bezpečná likvidácia
NIST SP 800-53 Rev.5	CP-9, CP-10, SI-12, MP-6	Požiadavky na systémové zálohovanie, obnovu a sanitizáciu médií
Nariadenie EÚ GDPR	Článok 32, Odôvodnenie 49	Obnova a dostupnosť osobných údajov, kontinuita činností
Smernica EÚ NIS2	Článok 21(2)(c-e)	Kontroly zálohovania a kontinuity na zabezpečenie odolnosti
Nariadenie EÚ DORA	Články 10, 11	Požiadavky finančného sektora na zálohovanie, obnovu a testovanie
COBIT 2019	DSS01, DSS04, MEA	Prevádzka zálohovania, kontinuita a priebežné monitorovanie súladu

1. Účel

1.1 Účelom tejto politiky je stanoviť záväzné požiadavky na zálohovanie a obnovu údajov, systémov a aplikácií na podporu prevádzkovej odolnosti, integrity údajov a kontinuity činností.

1.2 Táto politika stanovuje štandardizovaný rámec na:

1.2.1 ochranu údajov organizácie pred stratou v dôsledku vymazania, poškodenia, zlyhania alebo kybernetických útokov,

1.2.2 určenie požiadaviek na obnovu prostredníctvom jasne definovaných parametrov RTO (Recovery Time Objective) a RPO (Recovery Point Objective),

1.2.3 integráciu zálohovacích činností do širšieho systému manažérstva informačnej bezpečnosti (ISMS) a plánov kontinuity činností a obnovy po havárii (BCP/DRP),

1.2.4 zabezpečenie súladu s uplatniteľnými právnymi predpismi a odvetvovými reguláciami v oblasti dostupnosti a obnoviteľnosti.

1.3 Táto politika uplatňuje požiadavky ISO/IEC 27001:2022 týkajúce sa bezpečnej likvidácie údajov (5.28), odolnosti (5.29) a zálohovania informácií (8.13) a vychádza z osvedčených postupov podľa ISO/IEC 27002:2022, NIST SP 800-53 Rev.5, GDPR, DORA a NIS2.

2. Rozsah

2.1 Táto politika sa vzťahuje na:

2.1.1 všetky prevádzkovo kritické a kriticky dôležité systémy v rozsahu ISMS,

2.1.2 všetky štruktúrované a neštruktúrované údaje organizácie vrátane databáz, súborov, e-mailov a konfigurácií,

2.1.3 všetky prostredia — on-premise, cloudové, hybridné a vzdialené úložiská/úložiská mimo pracoviska,

2.1.4 všetkých pracovníkov zodpovedných za riadenie, vykonávanie, overovanie alebo obnovu procesov zálohovania.

2.2 Vzťahuje sa aj na:

2.2.1 zálohovacie médiá a infraštruktúru vrátane fyzických pások, virtuálnych zariadení, diskových snapshotov a cloudových riešení zálohovania,

2.2.2 poskytovateľov tretích strán zmluvne zabezpečujúcich hostovanie, správu alebo spracúvanie záloh organizácie,

2.2.3 zálohovanie logov, auditných stôp, konfigurácií a prevádzkovej dokumentácie kritickej pre kontinuitu činností.

2.3 Systémy výslovne vylúčené zo zálohovania musia byť zdokumentované, musia byť predmetom posúdenia rizík a ich vylúčenie musí formálne schváliť manažér ISMS a vlastník systému.

3. Ciele

3.1 Zabezpečiť, aby boli všetky kritické systémy a údaje spoľahlivo zálohované s dostatočnou frekvenciou, redundanciou a bezpečnostnými kontrolami.

3.2 Zaviesť mechanizmy obnovy, ktoré spĺňajú definované parametre RTO a RPO v súlade s analýzou vplyvu na podnikanie.

3.3 Udržiavať úplnú dokumentáciu postupov zálohovania, lehôt uchovávania, rolí a technológií.

3.4 Overovať účinnosť zálohovacích činností prostredníctvom systematického testovania obnovy, zaznamenávania zlyhaní a sledovania nápravných opatrení.

3.5 Chrániť zálohované údaje pred neoprávneným prístupom, zmenou alebo zničením počas celého ich životného cyklu.

3.6 Umožniť súlad s:

3.6.1 požiadavkami ISO/IEC 27001 na prevádzkové a kontinuálne kontroly,

3.6.2 rodinami kontrol NIST SP 800-53 CP a MP pre zálohovanie a sanitizáciu,

3.6.3 článkom 32 a odôvodnením 49 GDPR na obnovu prístupu k osobným údajom,

3.6.4 článkom 10 DORA a článkom 21 NIS2 na kontinuitu a odolnosť systémov IKT.

3.7 Zabezpečiť, aby služby zálohovania poskytované tretími stranami spĺňali zmluvné a regulačné bezpečnostné povinnosti vrátane šifrovania, likvidácie a notifikačných postupov.

4. Roly a zodpovednosti

4.1 Vrcholový manažment

4.1.1 schvaľuje túto politiku a zabezpečuje, aby boli kriticky dôležité systémy primerane chránené schválenými postupmi zálohovania a obnovy,

4.1.2 zodpovedá za zabezpečenie primeraných zdrojov na zálohovacie činnosti a ich pravidelné preskúmavanie z pohľadu súladu s regulačnými požiadavkami.

4.2 Riaditeľ informačnej bezpečnosti (CISO)

4.2.1 je vlastníkom tejto politiky a zabezpečuje jej zosúladenie so širším rámcom informačnej bezpečnosti, riadenia rizík a kontinuity,

4.2.2 dohliada na integráciu postupov zálohovania do BCP/DRP, reakcie na incidenty a plánovania odolnosti,

4.2.3 preskúmava výnimky zo zálohovania a posudzuje návrhy na akceptáciu rizika pri vylúčení kritických systémov.

[... 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 Táto politika sa musí preskúmať najmenej raz ročne alebo skôr, ak to vyvolá:

9.1.1 zmena stratégie kontinuity činností alebo obnovy po havárii,

9.1.2 nové regulačné alebo právne povinnosti ovplyvňujúce frekvenciu zálohovania alebo uchovávanie údajov,

9.1.3 zmeny architektúry systémov, nástrojov zálohovania alebo poskytovateľov služieb,

9.1.4 významné incidenty alebo auditné zistenia súvisiace so stratou údajov alebo zlyhaním obnovy.

9.2 Preskúmanie koordinuje CISO v spolupráci s:

9.2.1 tímom infraštruktúry a prevádzky IT,

9.2.2 tímom vnútorného auditu,

9.2.3 zodpovednou osobou pre ochranu osobných údajov (DPO),

9.2.4 tímami kontinuity činností a obnovy po havárii.

9.3 Harmonogramy zálohovania, zoznamy zahrnutých systémov, dokumentácia obnovy a záznamy o výnimkách sa musia preskúmavať súbežne s cieľom zabezpečiť:

9.3.1 správnosť pokrytia zálohovaním pre všetky kritické aktíva,

9.3.2 súlad s požiadavkami RTO/RPO a uchovávania,

9.3.3 úplnosť logov testovania a hlásení incidentov,

9.3.4 odstránenie predtým identifikovaných medzier v kontrolách.

9.4 Všetky aktualizácie musia:

9.4.1 podliehať riadeniu verzií a byť uchovávané v úložisku dokumentácie ISMS,

9.4.2 obsahovať zhrnutie zmien a odôvodnenie,

9.4.3 byť schválené vrcholovým manažmentom,

9.4.4 byť oznámené všetkým dotknutým technickým a prevádzkovým pracovníkom.

10. Súvisiace politiky a väzby

10.1 Táto politika priamo podporuje a súvisí s nasledujúcimi dokumentmi:

10.1.1 P6 – Politika riadenia rizík: Určuje prioritizáciu ochrany prostredníctvom zálohovania pre systémy a služby na základe rizík.

10.1.2 P12 – Politika správy aktív: Zabezpečuje, aby boli systémy vhodné na zálohovanie zahrnuté do inventarizácie aktív a prepojené so sledovaním životného cyklu a klasifikáciou.

10.1.3 P13 – Politika klasifikácie a označovania údajov: Usmerňuje, ktoré kategórie údajov vyžadujú zálohovanie vrátane označovania metadát na účely prioritizácie.

10.1.4 P14 – Politika uchovávania a likvidácie údajov: Koordinuje uchovávanie záloh s regulačnými limitmi uchovávania a správnou likvidáciou médií po uplynutí ich životnosti.

10.1.5 P16 – Politika maskovania údajov a pseudonymizácie: Podporuje minimalizáciu údajov pri zálohovaní citlivých dátových súborov.

10.1.6 P30 – Politika reakcie na incidenty: Aktivuje sa pri zlyhaniach zálohovania, problémoch s obnovou alebo kompromitácii úložísk zálohovaných údajov.

10.2 Tieto vzájomne prepojené politiky tvoria ucelený rámec, ktorý zabezpečuje, že správa a riadenie zálohovania je začlenená do širšieho ISMS a stratégie prevádzkovej odolnosti organizácie.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001:

11.1.1 Kapitola 6.1.3 – plán ošetrenia rizík: podporuje prioritizáciu zálohovania a plánovanie obnovy na základe rizík.

11.1.2 Kapitola 8.1 – prevádzkové plánovanie a riadenie: integruje kontroly obnovy a kontinuity ako súčasť prevádzkových opatrení.

11.1.3 Príloha A Kontrola 5.28 – bezpečná likvidácia alebo opätovné použitie zariadení: rieši bezpečnú sanitizáciu zálohovacích médií.

11.1.4 Príloha A Kontrola 5.29 – informačná bezpečnosť počas narušenia prevádzky: zabezpečuje schopnosti obnovy počas incidentov alebo havárií.

11.1.5 Príloha A Kontrola 8.13 – zálohovanie informácií: priamo riešené prostredníctvom plánovaných, testovaných a bezpečných zálohovacích činností.

11.2 ISO/IEC 27002:2022 – Kontroly 8.13, 5.28, 5.: Tieto kontroly posilňujú požiadavku na pravidelné zálohovanie, validáciu integrity a plánovanie obnovy vo všetkých IT prostrediach.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-9 – systémové zálohovanie: stanovuje komplexné postupy zálohovania vrátane ukladania mimo pracoviska a testovania obnovy.

11.3.2 CP-10 – obnova a rekonštrukcia systému: vyžaduje validované postupy pre úplnú alebo čiastočnú obnovu v súlade s cieľmi obnovy.

11.3.3 MP-6 – sanitizácia médií: zabezpečuje bezpečné nakladanie so zastaranými zálohovacími médiami.

11.3.4 SI-12 – postupy pri nakladaní s informáciami: posilňuje zodpovednosti za zálohovanie a obnovu citlivých údajov.

11.4 Nariadenie EÚ GDPR (2016/679):

11.4.1 Článok 32 – bezpečnosť spracúvania: ukladá povinnosť zabezpečiť schopnosti obnovy a opatrenia na zabezpečenie dostupnosti údajov, najmä pri osobných údajoch.

11.4.2 Odôvodnenie 49: podporuje opatrenia kontinuity činností a obnovy po havárii vrátane bezpečného zálohovania ako súčasti odolnosti organizácie.

11.5 Smernica EÚ NIS2 (2022/2555):

11.5.1 Článok 21(2)(c-e): vyžaduje technické a organizačné opatrenia vrátane kontrol zálohovania a kontinuity na zabezpečenie odolnosti služieb.

11.6 Nariadenie EÚ DORA (2022/2554):

11.6.1 Článok 10 – kontinuita činností IKT: vyžaduje, aby finančné subjekty mali zavedené úplné zálohovanie údajov, obnovu a plánovanie kontinuity.

11.6.2 Článok 11 – testovanie plánov kontinuity činností IKT: zdôrazňuje validáciu schopnosti obnovy prostredníctvom pravidelného testovania.

11.7 COBIT 2019:

11.7.1 DSS01 – riadené prevádzkové činnosti: podporuje spoľahlivé poskytovanie služieb prostredníctvom chránenej dostupnosti údajov.

11.7.2 DSS04 – riadená kontinuita: definuje strategické a prevádzkové kontroly kontinuity vrátane overených záloh.

11.7.3 MEA03 – Monitorovanie, hodnotenie a posudzovanie súladu: vyžaduje pravidelné preskúmavanie opatrení kontinuity vrátane účinnosti kontrol zálohovania.