					Sem vložte název registrované právnické osoby						
Číslo dokumentu: P15					Název dokumentu: **Politika zálohování a obnovy**						
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	Kapitoly 6.1.3, 8	Ošetření rizik, plánování a provozní opatření pro zálohování
ISO/IEC 27002:2022	Opatření 8.13, 5.28, 5.29	Řízení zálohování, bezpečná likvidace a odolnost
NIST SP 800-53 Rev.5	CP-9, CP-10, SI-12, MP-6	Požadavky na zálohování systémů, obnovu a sanitizaci médií
GDPR	Článek 32, bod odůvodnění 49	Obnova a dostupnost osobních údajů, kontinuita činností
směrnice NIS2	Článek 21(2)(c-e)	Opatření v oblasti zálohování a kontinuity pro zajištění odolnosti
nařízení DORA	Články 10, 11	Požadavky finančního sektoru na zálohování, obnovu a testování
COBIT 2019	DSS01, DSS04, MEA03	Provoz zálohování, kontinuita a monitorování souladu

1. Účel

1.1 Účelem této politiky je stanovit závazné požadavky na zálohování a obnovu dat, systémů a aplikací za účelem podpory provozní odolnosti, integrity dat a kontinuity činností.

1.2 Tato politika zavádí standardizovaný rámec pro:

1.2.1 ochranu dat organizace před ztrátou v důsledku smazání, poškození, selhání nebo kybernetických útoků,

1.2.2 stanovení požadavků na obnovu prostřednictvím jasně definovaných parametrů RTO (Recovery Time Objective) a RPO (Recovery Point Objective),

1.2.3 integraci činností zálohování do širšího systému řízení bezpečnosti informací (ISMS) a plánů kontinuity činností a obnovy po havárii (BCP/DRP),

1.2.4 zajištění souladu s příslušnými právními předpisy a sektorovými regulačními požadavky na dostupnost a obnovitelnost.

1.3 Tato politika zavádí opatření normy ISO/IEC 27001:2022 související s bezpečnou likvidací dat (5.28), odolností (5.29) a zálohováním informací (8.13) a vychází z osvědčených postupů norem ISO/IEC 27002:2022, NIST SP 800-53 Rev.5, GDPR, nařízení DORA a směrnice NIS2.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 všechny systémy kritické pro podnikání a provozní systémy v rozsahu ISMS,

2.1.2 veškerá strukturovaná i nestrukturovaná podniková data, včetně databází, souborů, e-mailů a konfigurací,

2.1.3 všechna prostředí — on-premise, cloudová, hybridní a vzdálená úložiště / úložiště mimo pracoviště,

2.1.4 veškerý personál odpovědný za řízení, provádění, ověřování nebo obnovu procesů zálohování.

2.2 Vztahuje se rovněž na:

2.2.1 zálohovací média a infrastrukturu, včetně fyzických pásek, virtuálních zařízení, diskových snapshotů a cloudových řešení zálohování,

2.2.2 poskytovatele služeb třetích stran, kteří smluvně zajišťují hostování, správu nebo zpracování záloh organizace,

2.2.3 zálohování logů, konfigurací, auditních stop a provozní dokumentace kritické pro kontinuitu.

2.3 Systémy výslovně vyloučené ze zálohování musí být zdokumentovány, podrobeny hodnocení rizik a formálně schváleny manažerem ISMS a vlastníkem systému.

3. Cíle

3.1 Zajistit, aby všechny kritické systémy a data byly spolehlivě zálohovány s dostatečnou frekvencí, redundancí a bezpečnostními opatřeními.

3.2 Zajistit mechanismy obnovy, které splňují stanovené požadavky RTO a RPO v souladu s analýzou dopadů na podnikání.

3.3 Udržovat úplnou dokumentaci postupů zálohování, harmonogramů uchovávání, rolí a používaných technologií.

3.4 Ověřovat účinnost činností zálohování prostřednictvím systematického testování obnovy, zaznamenávání selhání a sledování nápravných opatření.

3.5 Chránit zálohovaná data před neoprávněným přístupem, změnou nebo zničením po celou dobu jejich životního cyklu.

3.6 Umožnit soulad s:

3.6.1 požadavky ISO/IEC 27001 na provozní opatření a kontinuitu,

3.6.2 rodinami opatření NIST SP 800-53 CP a MP pro zálohování a sanitizaci,

3.6.3 článkem 32 GDPR a bodem odůvodnění 49 GDPR pro obnovení přístupu k osobním údajům,

3.6.4 článkem 10 nařízení DORA a článkem 21 směrnice NIS2 pro kontinuitu a odolnost v oblasti ICT.

3.7 Zajistit, aby služby zálohování poskytované třetími stranami splňovaly smluvní a regulační bezpečnostní povinnosti, včetně šifrování, likvidace a oznamovacích postupů.

4. Role a odpovědnosti

4.1 Vrcholové vedení

4.1.1 schvaluje tuto politiku a zajišťuje, aby systémy kritické pro podnikání byly odpovídajícím způsobem chráněny schválenými postupy zálohování a obnovy,

4.1.2 odpovídá za zajištění dostatečných zdrojů pro činnosti zálohování a za jejich pravidelný přezkum z hlediska souladu s regulačními požadavky.

4.2 Ředitel informační bezpečnosti (CISO)

4.2.1 je vlastníkem této politiky a zajišťuje její soulad s širším rámcem bezpečnosti informací, řízení rizik a kontinuity činností,

4.2.2 dohlíží na začlenění postupů zálohování do BCP/DRP, reakce na incidenty a plánování odolnosti,

4.2.3 přezkoumává výjimky v oblasti zálohování a vyhodnocuje návrhy na přijetí rizika pro vyloučení kritických systémů.

[... 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 přezkoumána nejméně jednou ročně nebo dříve, pokud to vyvolá:

9.1.1 změna strategie kontinuity činností nebo obnovy po havárii,

9.1.2 nová regulační nebo právní povinnost ovlivňující frekvenci zálohování nebo uchovávání dat,

9.1.3 změny architektury systémů, nástrojů zálohování nebo poskytovatelů služeb,

9.1.4 významné incidenty nebo zjištění auditu související se ztrátou dat nebo selháním obnovy.

9.2 Přezkum koordinuje CISO ve spolupráci s:

9.2.1 IT infrastrukturou a provozem,

9.2.2 interním auditem,

9.2.3 pověřencem pro ochranu osobních údajů,

9.2.4 týmy kontinuity činností a obnovy po havárii.

9.3 Harmonogramy zálohování, seznamy zahrnutých systémů, dokumentace obnovy a logy výjimek musí být přezkoumávány souběžně, aby bylo zajištěno:

9.3.1 přesné pokrytí zálohováním pro všechna kritická aktiva,

9.3.2 soulad s požadavky RTO/RPO a uchovávání,

9.3.3 úplnost logů testování a hlášení incidentů,

9.3.4 náprava dříve identifikovaných mezer v kontrolách.

9.4 Všechny aktualizace musí:

9.4.1 být vedeny ve verzovaném režimu a uchovávány v repozitáři dokumentace ISMS,

9.4.2 obsahovat souhrn změn a jejich odůvodnění,

9.4.3 být schváleny vrcholovým vedením,

9.4.4 být komunikovány všem dotčeným technickým i obchodním pracovníkům.

10. Související politiky a vazby

10.1 Tato politika přímo podporuje následující související dokumenty a navazuje na ně:

10.1.1 P6 - Politika řízení rizik: určuje prioritu ochrany záloh systémů a služeb na základě rizik.

10.1.2 P12 - Politika správy aktiv: zajišťuje, že systémy způsobilé k zálohování jsou evidovány a navázány na sledování životního cyklu a klasifikaci.

10.1.3 P13 - Politika klasifikace a označování dat: určuje, které kategorie dat vyžadují zálohování, včetně klasifikačních metadat pro prioritizaci.

10.1.4 P14 - Politika uchovávání a likvidace dat: koordinuje uchovávání záloh s regulačními limity uchovávání a správnou likvidací expirovaných médií.

10.1.5 P16 - Politika maskování dat a pseudonymizace: podporuje minimalizaci dat při zálohování citlivých datových sad.

10.1.6 P30 - Politika reakce na incidenty: aktivuje se při selhání zálohování, problémech s obnovou nebo kompromitaci repozitářů zálohovaných dat.

10.2 Tyto vzájemně provázané politiky tvoří soudržný rámec, který zajišťuje, že správa a řízení zálohování je začleněna do širší strategie ISMS a provozní odolnosti organizace.

11. Referenční normy a rámce

11.1 ISO/IEC 27001:

11.1.1 Kapitola 6.1.3 - Plán ošetření rizik: podporuje prioritizaci zálohování a plánování obnovy na základě rizik.

11.1.2 Kapitola 8.1 - Provozní plánování a řízení: integruje opatření obnovy a kontinuity jako součást provozních bezpečnostních opatření.

11.1.3 Příloha A, opatření 5.28 - Bezpečná likvidace nebo opětovné použití zařízení: řeší bezpečnou sanitizaci zálohovacích médií.

11.1.4 Příloha A, opatření 5.29 - Bezpečnost informací během narušení: zajišťuje schopnosti obnovy během incidentů nebo havárií.

11.1.5 Příloha A, opatření 8.13 - Zálohování informací: je přímo řešeno prostřednictvím plánovaných, testovaných a bezpečných činností zálohování.

11.2 ISO/IEC 27002:2022 - Opatření 8.13, 5.28, 5.29: Tato opatření posilují požadavek na pravidelné zálohování, validaci integrity a plánování obnovy napříč všemi IT prostředími.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-9 - Zálohování systému: stanovuje komplexní postupy zálohování včetně ukládání mimo lokalitu a testování obnovy.

11.3.2 CP-10 - Obnova a restaurování systému: vyžaduje validované postupy pro úplnou nebo částečnou obnovu v souladu s cíli obnovy.

11.3.3 MP-6 - Sanitizace médií: zajišťuje bezpečné nakládání se zastaralými zálohovacími médii.

11.3.4 SI-12 - Postupy nakládání s informacemi: posiluje odpovědnosti za zálohování a obnovu citlivých dat.

11.4 GDPR (2016/679):

11.4.1 Článek 32 - Zabezpečení zpracování: ukládá povinnost zajistit schopnosti obnovy a opatření pro dostupnost dat, zejména osobních údajů.

11.4.2 Bod odůvodnění 49: podporuje opatření kontinuity činností a obnovy po havárii, včetně bezpečného zálohování jako součásti odolnosti organizace.

11.5 Směrnice NIS2 (2022/2555):

11.5.1 Článek 21(2)(c-e): vyžaduje technická a organizační opatření, včetně zálohování a opatření kontinuity, k zajištění odolnosti služeb.

11.6 Nařízení DORA (2022/2554):

11.6.1 Článek 10 - Kontinuita činností v oblasti ICT: vyžaduje, aby finanční subjekty měly úplné zálohování dat, obnovu a plánování kontinuity.

11.6.2 Článek 11 - Testování plánů kontinuity činností v oblasti ICT: zdůrazňuje ověřování schopností obnovy prostřednictvím pravidelného testování.

11.7 COBIT 2019:

11.7.1 DSS01 - Řízený provoz: podporuje spolehlivé poskytování služeb prostřednictvím chráněné dostupnosti dat.

11.7.2 DSS04 - Řízená kontinuita: vymezuje strategická a provozní opatření kontinuity včetně ověřených záloh.

11.7.3 MEA03 - Monitorování, vyhodnocování a posuzování souladu: ukládá pravidelný přezkum opatření kontinuity včetně účinnosti opatření zálohování.