| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sem vložte název registrované právnické osoby | | | | | | |
| Číslo dokumentu:<br>P15S | | | | | Název dokumentu:<br>**Politika zálohování a obnovy** | | | | | | |
| Verze:<br>1.0 | | Datum účinnosti:<br>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 | Ustanovení/článek | Komentář |
|---|---|---|
| ISO/IEC 27001:2022 | Kapitola 8 | Opatření pro zálohování podle požadavků ISMS |
| ISO/IEC 27002:2022 | Opatření 5.29, 8.13 | Osvědčené postupy pro zálohování a integrace s kontinuitou činností |
| NIST SP 800-53 Rev.5 | CP-9, MP-6 | Zálohování a ochrana médií |
| EU NIS2 | Článek 21(2)(c) | Odolnost a kontinuita prostřednictvím zálohování |
| EU DORA | Článek 10(1) | Kontinuita ICT – zálohování pro finanční instituce |
| COBIT 2019 | BAI04.05, DSS04 | Dokumentace a testování záloh, řízení kontrolních procesů |
| GDPR | Články 5(1)(f), 32(1)(c) | Integrita, dostupnost a včasná obnova dat |

**1. Účel**

1.1 Tato politika stanoví způsob provádění a řízení zálohování v organizaci tak, aby byla zajištěna kontinuita činností, ochrana před ztrátou dat a včasná obnova po incidentech.

1.2 Stanoví závazná pravidla pro zálohování, ukládání a obnovu systémů a dat, zejména v prostředí SME bez komplexní IT infrastruktury.

1.3 Tato politika podporuje připravenost na audit a certifikaci podle ISO/IEC 27001 tím, že zajišťuje zavedení, konzistentní uplatňování a pravidelný přezkum nezbytných opatření pro zálohování.

1.4 Schopnost organizace obnovit provoz po technických selháních, neúmyslném smazání nebo kybernetických incidentech závisí na důsledném dodržování této politiky.

**2. Rozsah**

**2.1 Tato politika se vztahuje na všechny podnikové systémy a data, včetně:**

2.1.1 finančních záznamů, informací o zákaznících a personálních údajů,

2.1.2 stolních počítačů, notebooků, serverů a cloudových aplikací používaných při obchodních činnostech,

2.1.3 záložních médií, jako jsou USB disky, externí úložiště nebo cloudové zálohy.

**2.2 Vztahuje se rovněž na všechny osoby odpovědné za provádění nebo řízení procesů zálohování, včetně:**

2.2.1 generálního ředitele (GM) nebo určené odpovědné osoby,

2.2.2 externích poskytovatelů IT podpory nebo konzultantů,

2.2.3 všech zaměstnanců odpovědných za ukládání dat do schválených umístění.

**3. Cíle**

3.1 Zajistit, aby všechna kritická data a systémy nezbytné pro podnikání byly bezpečně zálohovány ve vhodných intervalech podle rizika a provozních potřeb.

3.2 Zajistit, aby data mohla být po narušení obnovena včas a úplně.

3.3 Zabránit neoprávněnému přístupu, manipulaci nebo ztrátě záložních dat prostřednictvím účinných kontrol ukládání.

3.4 Jednoznačně přiřadit a vynucovat role a odpovědnosti za implementaci a testování postupů zálohování.

3.5 Podporovat soulad s ISO/IEC 27001, GDPR a dalšími regulačními požadavky prostřednictvím strukturovaných a dokumentovaných postupů zálohování.

**4. Role a odpovědnosti**

**4.1 Generální ředitel (GM)**

4.1.1 schvaluje tuto politiku a zajišťuje její uplatňování,

4.1.2 přiděluje zdroje a určuje odpovědnost za činnosti zálohování a obnovy,

4.1.3 přezkoumává selhání zálohování, incidenty nebo odchylky od této politiky,

4.1.4 řídí každoroční přezkum politiky a zajišťuje připravenost na audit.

**4.2 Externí poskytovatel IT podpory (je-li relevantní)**

4.2.1 zavádí a spravuje řešení zálohování (lokálně nebo v cloudu),

4.2.2 monitoruje úspěšnost zálohování a plánuje testy obnovy,

4.2.3 hlásí selhání a incidenty přímo GM,

4.2.4 zajišťuje šifrování, omezení přístupu a řádné nakládání se záložními médii.

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

**9. Požadavky na přezkum a aktualizaci**

**9.1 Tato politika musí být přezkoumána GM nejméně jednou ročně. Spouštěče průběžného přezkumu zahrnují:**

9.1.1 významné změny systémů nebo metod ukládání,

9.1.2 zavedení nových cloudových nebo IT platforem,

9.1.3 právní nebo regulatorní změny ovlivňující obnovu dat,

9.1.4 zjištění z auditů nebo incidenty.

9.2 GM odpovídá za zahájení přezkumu, schválení změn a komunikaci aktualizací.

9.3 Verze politiky musí být evidovány a archivovány. Nahrazené verze musí mít omezený přístup, aby se předešlo nejasnostem během auditů nebo událostí souvisejících s obnovou provozu.

**10. Související politiky a vazby**

**10.1 Tato politika je v souladu s následujícími politikami SME a navazuje na ně:**

10.1.1 P14S – Politika uchovávání údajů: stanoví, jak dlouho mají být záložní data uchovávána a jak mají být bezpečně mazána.

10.1.2 P13S – Politika klasifikace dat a označování: pomáhá určit prioritu dat, která musí být zálohována podle úrovně klasifikace.

10.1.3 P30S – Politika reakce na incidenty: upravuje postupy pro případy selhání záloh nebo potřeby obnovy dat po bezpečnostním incidentu nebo výpadku.

10.1.4 P2S – Politika rolí a odpovědností v oblasti správy a řízení: přiřazuje jednoznačnou pravomoc pro dohled nad zálohováním a uplatňování politiky.

10.1.5 P17S – Politika ochrany dat a soukromí: zajišťuje, aby nakládání se zálohami obsahujícími osobní údaje bylo v souladu s právními předpisy a požadavky na ochranu soukromí.

**11. Referenční normy a rámce**

**11.1 ISO/IEC 27001**

11.1.1 Kapitola 8.1: provozní plánování a řízení záložních systémů jako součásti ISMS.

**11.2 ISO/IEC 27002**

11.2.1 Opatření 8.13: stanoví osvědčené postupy pro plánování zálohování, monitorování a obnovu.

11.2.2 Příloha A, opatření 5.29: integrace zálohování s kontinuitou činností a připraveností na obnovu.

**11.3 NIST SP 800-53 Rev.5**

11.3.1 CP-9 (Contingency Planning): definuje strukturované strategie zálohování pro odolnost organizace.

11.3.2 MP-6 (Media Protection): vyžaduje bezpečné nakládání se záložními médii a jejich likvidaci.

**11.4 GDPR**

11.4.1 Článek 5(1)(f): stanoví požadavek na integritu a dostupnost osobních údajů.

11.4.2 Článek 32(1)(c): vyžaduje schopnost včas obnovit přístup k osobním údajům.

**11.5 Směrnice NIS2**

11.5.1 Článek 21(2)(c): vyžaduje zálohování a obnovu jako součást plánování odolnosti a kontinuity.

**11.6 Nařízení DORA**

11.6.1 Článek 10(1): organizace ve finančním sektoru musí zajistit zálohování jako součást opatření pro kontinuitu ICT.

**11.7 COBIT 2019**

11.7.1 BAI04.05: vyžaduje dokumentované strategie zálohování.

11.7.2 DSS04.07: zdůrazňuje pravidelné testování a řízení procesů zálohování a obnovy dat.