					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P15S					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**

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitola 8	Kontroly zálohovania podľa požiadaviek ISMS
ISO/IEC 27002:2022	Kontroly 5.29, 8	Osvedčené postupy zálohovania a integrácia s kontinuitou činností
NIST SP 800-53 Rev. 5	CP-9, MP-6	Zálohovanie a ochrana médií
Smernica EÚ NIS2	Článok 21(2)(c)	Odolnosť a kontinuita prostredníctvom zálohovania
Nariadenie EÚ DORA	Článok 10(1)	Kontinuita systémov IKT – zálohovanie pre organizácie finančného sektora
COBIT 2019	BAI04.05, DSS04	Dokumentovanie a testovanie záloh, riadenie procesov
Nariadenie EÚ GDPR	Články 5(1)(f), 32(1)(c)	Integrita, dostupnosť a včasná obnova údajov

1. Účel

1.1 Táto politika stanovuje, ako organizácia vykonáva a riadi zálohovanie s cieľom zabezpečiť kontinuitu činností, chrániť pred stratou údajov a umožniť včasnú obnovu po incidentoch.

1.2 Stanovuje záväzné pravidlá pre zálohovanie, uchovávanie a obnovu systémov a údajov, najmä v malých a stredných podnikoch bez komplexnej IT infraštruktúry.

1.3 Táto politika podporuje pripravenosť na audit a certifikáciu podľa ISO/IEC 27001 tým, že zabezpečuje zavedenie nevyhnutných kontrol zálohovania, ich konzistentné uplatňovanie a pravidelné preskúmavanie.

1.4 Schopnosť organizácie obnoviť prevádzku po technických zlyhaniach, náhodnom vymazaní alebo kybernetických incidentoch závisí od dôsledného dodržiavania tejto politiky.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky podnikové systémy a údaje vrátane:

2.1.1 finančných záznamov, informácií o zákazníkoch a personálnych údajov,

2.1.2 stolových počítačov, notebookov, serverov a cloudových aplikácií používaných v prevádzke organizácie,

2.1.3 zálohovacích médií, ako sú USB disky, externé úložiská alebo zálohy v cloudovom prostredí.

2.2 Vzťahuje sa aj na všetky osoby zodpovedné za vykonávanie alebo riadenie procesov zálohovania vrátane:

2.2.1 generálneho manažéra (GM) alebo určenej zodpovednej osoby,

2.2.2 externých poskytovateľov IT podpory alebo konzultantov,

2.2.3 všetkých zamestnancov zodpovedných za ukladanie údajov do schválených umiestnení.

3. Ciele

3.1 Zabezpečiť, aby všetky kritické údaje a systémy organizácie boli bezpečne zálohované v primeraných intervaloch na základe rizika a prevádzkových potrieb.

3.2 Zabezpečiť, že údaje bude možné po narušení obnoviť včas a v úplnom rozsahu.

3.3 Predchádzať neoprávnenému prístupu, manipulácii alebo strate zálohovaných údajov prostredníctvom účinných kontrol uchovávania.

3.4 Jednoznačne priradiť a uplatňovať roly a zodpovednosti za vykonávanie a testovanie postupov zálohovania.

3.5 Podporovať súlad s ISO/IEC 27001, GDPR a ďalšími regulačnými požiadavkami prostredníctvom štruktúrovaných a zdokumentovaných postupov zálohovania.

4. Roly a zodpovednosti

4.1 Generálny manažér (GM)

4.1.1 schvaľuje túto politiku a zabezpečuje jej uplatňovanie,

4.1.2 prideľuje zdroje a určuje zodpovednosť za činnosti zálohovania a obnovy,

4.1.3 preskúmava zlyhania zálohovania, incidenty alebo odchýlky od politiky,

4.1.4 vykonáva ročné preskúmanie politiky a zabezpečuje pripravenosť na audit.

4.2 Externý poskytovateľ IT podpory (ak je relevantné)

4.2.1 zavádza a riadi riešenia zálohovania (lokálne alebo v cloudovom prostredí),

4.2.2 monitoruje úspešnosť zálohovania a plánuje testy obnovy,

4.2.3 nahlasuje zlyhania a incidenty priamo GM,

4.2.4 zabezpečuje šifrovanie, obmedzenie prístupu a správne nakladanie so zálohovacími médiami.

[... 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 GM preskúmať najmenej raz ročne. Spúšťače priebežného preskúmania zahŕňajú:

9.1.1 významné zmeny systémov alebo metód uchovávania,

9.1.2 zavedenie nových cloudových alebo IT platforiem,

9.1.3 právne alebo regulačné zmeny ovplyvňujúce obnovu údajov,

9.1.4 zistenia z auditov alebo incidentov.

9.2 GM zodpovedá za iniciovanie preskúmania, schválenie zmien a komunikovanie aktualizácií.

9.3 Verzie politiky musia byť sledované a archivované. Nahradené verzie musia mať obmedzený prístup, aby sa predišlo nejasnostiam počas auditov alebo udalostí súvisiacich s obnovou činností organizácie.

10. Súvisiace politiky a väzby

10.1 Táto politika je v súlade s nasledujúcimi SME politikami a nadväzuje na ne:

10.1.1 P14S – Politika uchovávania a likvidácie údajov: stanovuje, ako dlho sa majú uchovávať zálohované údaje a ako sa majú bezpečne vymazávať.

10.1.2 P13S – Politika klasifikácie a označovania údajov: pomáha určiť priority zálohovania údajov podľa úrovne klasifikácie.

10.1.3 P30S – Politika reakcie na incidenty: upravuje postupy pre prípady zlyhania záloh alebo potreby obnovy údajov po porušení alebo výpadku.

10.1.4 P2S – Politika rolí a zodpovedností v oblasti správy a riadenia: prideľuje jasné právomoci na dohľad nad zálohovaním a uplatňovanie politiky.

10.1.5 P17S – Politika ochrany údajov a súkromia: zabezpečuje, aby nakladanie so zálohami obsahujúcimi osobné údaje bolo v súlade so zákonnými požiadavkami a požiadavkami na ochranu súkromia.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 8.1: prevádzkové plánovanie a riadenie zálohovacích systémov ako súčasť ISMS.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.13: stanovuje osvedčené postupy pre plánovanie zálohovania, monitorovanie a obnovu.

11.2.2 Príloha A, kontrola 5.29: integrácia zálohovania s kontinuitou činností a pripravenosťou na obnovu.

11.3 NIST SP 800-53 Rev. 5

11.3.1 CP-9 (plánovanie pre nepredvídané udalosti): stanovuje štruktúrované stratégie zálohovania na podporu odolnosti organizácie.

11.3.2 MP-6 (ochrana médií): vyžaduje bezpečné nakladanie so zálohovacími médiami a ich likvidáciu.

11.4 Nariadenie EÚ GDPR

11.4.1 Článok 5(1)(f): vyžaduje integritu a dostupnosť osobných údajov.

11.4.2 Článok 32(1)(c): vyžaduje schopnosť včas obnoviť prístup k osobným údajom.

11.5 Smernica EÚ NIS2

11.5.1 Článok 21(2)(c): vyžaduje zálohovanie a obnovu ako súčasť plánovania odolnosti a kontinuity.

11.6 Nariadenie EÚ DORA

11.6.1 Článok 10(1): organizácie finančného sektora musia zabezpečiť zálohovanie ako súčasť opatrení kontinuity systémov IKT.

11.7 COBIT 2019

11.7.1 BAI04.05: vyžaduje zdokumentované stratégie zálohovania.

11.7.2 DSS04.07: zdôrazňuje pravidelné testovanie a riadenie procesov zálohovania a obnovy údajov.