					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P15S					Naslov dokumenta: **Politika varnostnega kopiranja in obnove**							
Različica: 1.0		Datum začetka veljavnosti: 01.01.2025			Lastnik dokumenta:							
X	Politika		Standard		Postopek		Obrazec		Register		Drugo	

Zgodovina revizij				
Številka revizije	**Datum revizije**	**Spremembe**	**Pregledal**	**Lastnik procesa**

Odobritve			
Ime	**Delovno mesto**	**Datum**	**Podpis**

Pravno obvestilo (avtorske pravice in omejitve uporabe)

(C) 2025 Clarysec LLC. All rights reserved.

Ta dokument je intelektualna lastnina družbe Clarysec LLC. Noben del tega dokumenta se ne sme kopirati, ponovno uporabiti, distribuirati ali spreminjati za komercialne ali implementacijske namene brez predhodnega izrecnega pisnega dovoljenja.

Nepooblaščena uporaba je strogo prepovedana in lahko povzroči pravne ukrepe.

Za licenciranje se obrnite na: info@clarysec.com

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
ISO/IEC 27001:2022	Klavzula 8	Kontrole varnostnega kopiranja v skladu z zahtevami ISMS
ISO/IEC 27002:2022	Kontroli 5.29, 8.13	Dobre prakse za varnostno kopiranje in povezava z neprekinjenim poslovanjem
NIST SP 800-53 Rev. 5	CP-9, MP-6	Varnostno kopiranje in zaščita medijev
Direktiva EU NIS2	Člen 21(2)(c)	Odpornost in neprekinjeno poslovanje z varnostnim kopiranjem
Uredba EU DORA	Člen 10(1)	Neprekinjenost IKT – varnostno kopiranje za finančne organizacije
COBIT 2019	BAI04.05, DSS04	Dokumentiranje in testiranje varnostnih kopij ter kontrola procesov
EU GDPR	Člena 5(1)(f), 32(1)(c)	Celovitost, razpoložljivost in pravočasna obnova podatkov

1. Namen

1.1 Ta politika določa, kako organizacija izvaja in upravlja varnostno kopiranje, da zagotovi neprekinjeno poslovanje, zaščiti podatke pred izgubo ter omogoči pravočasno obnovo po incidentih.

1.2 Določa zavezujoča pravila za varnostno kopiranje, hrambo in obnovo sistemov ter podatkov, zlasti v malih in srednje velikih podjetjih brez kompleksne IT-infrastrukture.

1.3 Ta politika podpira pripravljenost na presojo in certificiranje po standardu ISO/IEC 27001, saj zagotavlja vzpostavljene, dosledno uporabljane in redno pregledovane bistvene kontrole varnostnega kopiranja.

1.4 Sposobnost organizacije za obnovo po tehničnih okvarah, nenamernem izbrisu ali kibernetskih incidentih je odvisna od doslednega upoštevanja te politike.

2. Področje uporabe

2.1 Ta politika se uporablja za vse poslovne sisteme in podatke, vključno z:

2.1.1 finančnimi evidencami, podatki o strankah in kadrovskimi podatki,

2.1.2 namiznimi računalniki, prenosniki, strežniki in aplikacijami v oblaku, ki se uporabljajo pri poslovanju,

2.1.3 mediji za varnostno kopiranje, kot so ključki USB, zunanje naprave za shranjevanje ali varnostne kopije v oblaku.

2.2 Uporablja se tudi za vse posameznike, odgovorne za izvajanje ali upravljanje postopkov varnostnega kopiranja, vključno z:

2.2.1 glavnim direktorjem (GM) ali drugo imenovano odgovorno osebo,

2.2.2 zunanjimi ponudniki IT-podpore ali svetovalci,

2.2.3 vsemi zaposlenimi, odgovornimi za shranjevanje podatkov na odobrenih lokacijah.

3. Cilji

3.1 Zagotoviti, da se vsi ključni poslovni podatki in sistemi varnostno kopirajo varno in v ustreznih intervalih glede na tveganja ter operativne potrebe.

3.2 Zagotoviti, da se podatki po motnjah lahko obnovijo pravočasno in v celoti.

3.3 Preprečiti nepooblaščen dostop, nepooblaščene spremembe ali izgubo podatkov iz varnostnih kopij z učinkovitimi kontrolami hrambe.

3.4 Jasno določiti in uveljavljati vloge ter odgovornosti za izvajanje in testiranje postopkov varnostnega kopiranja.

3.5 Podpreti skladnost z ISO/IEC 27001, GDPR in drugimi regulativnimi obveznostmi s strukturiranimi in dokumentiranimi praksami varnostnega kopiranja.

4. Vloge in odgovornosti

4.1 Glavni direktor (GM)

4.1.1 odobri to politiko in zagotovi njeno izvajanje,

4.1.2 dodeli vire in določi odgovornosti za dejavnosti varnostnega kopiranja in obnove,

4.1.3 pregleduje napake pri varnostnem kopiranju, incidente ali odstopanja od politike,

4.1.4 izvaja letne preglede politike in zagotavlja pripravljenost na presojo.

4.2 Zunanji ponudnik IT-podpore (če je v uporabi)

4.2.1 vzpostavi in upravlja rešitve za varnostno kopiranje (lokalne ali v oblaku),

4.2.2 spremlja uspešnost varnostnega kopiranja in načrtuje teste obnove,

4.2.3 o napakah in incidentih neposredno poroča GM,

4.2.4 zagotavlja šifriranje, omejitve dostopa in ustrezno ravnanje z mediji za varnostno kopiranje.

[... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ...]

9. Zahteve za pregled in posodobitev

9.1 To politiko mora GM pregledati najmanj enkrat letno. Povodi za vmesni pregled vključujejo:

9.1.1 večje spremembe sistemov ali metod hrambe,

9.1.2 uvedbo novih storitev v oblaku ali IT-platform,

9.1.3 pravne ali regulativne spremembe, ki vplivajo na obnovo podatkov,

9.1.4 ugotovitve presoje ali incidente.

9.2 GM je odgovoren za začetek pregleda, odobritev sprememb in obveščanje o posodobitvah.

9.3 Različice politike morajo biti sledljive in arhivirane. Nadomeščene različice morajo imeti omejen dostop, da se prepreči zmeda med presojami ali dogodki poslovne obnove.

10. Povezane politike in povezave

10.1 Ta politika je usklajena z naslednjimi politikami SME in je od njih odvisna:

10.1.1 P14S – Politika hrambe podatkov in odstranjevanja: določa, kako dolgo se podatki iz varnostnih kopij hranijo in kako se varno izbrišejo.

10.1.2 P13S – Politika klasifikacije in označevanja podatkov: pomaga določiti prednostne podatke za varnostno kopiranje na podlagi ravni klasifikacije.

10.1.3 P30S – Politika odzivanja na incidente: določa postopke, če varnostno kopiranje odpove ali če je po kršitvi ali izpadu potrebna obnova podatkov.

10.1.4 P2S – Politika vlog in odgovornosti upravljanja: določa jasna pooblastila za nadzor nad varnostnim kopiranjem in izvajanje politike.

10.1.5 P17S – Politika varstva podatkov in zasebnosti: zagotavlja, da je ravnanje z osebnimi podatki v varnostnih kopijah usklajeno s pravnimi zahtevami in zahtevami glede zasebnosti.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 8.1: operativno načrtovanje in kontrola sistemov varnostnega kopiranja kot dela ISMS.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.13: določa dobre prakse za načrtovanje, spremljanje in obnovo varnostnih kopij.

11.2.2 Priloga A, Kontrola 5.29: povezava varnostnega kopiranja z neprekinjenim poslovanjem in pripravljenostjo na obnovo.

11.3 NIST SP 800-53 Rev. 5

11.3.1 CP-9 (Contingency Planning): določa strukturirane strategije varnostnega kopiranja za poslovno odpornost.

11.3.2 MP-6 (Media Protection): zahteva varno ravnanje z mediji za varnostno kopiranje in njihovo uničenje.

11.4 EU GDPR

11.4.1 Člen 5(1)(f): zahteva celovitost in razpoložljivost osebnih podatkov.

11.4.2 Člen 32(1)(c): zahteva zmožnost pravočasne obnove dostopa do osebnih podatkov.

11.5 Direktiva EU NIS2

11.5.1 Člen 21(2)(c): zahteva varnostno kopiranje in obnovo kot del načrtovanja odpornosti in neprekinjenega poslovanja.

11.6 Uredba EU DORA

11.6.1 Člen 10(1): organizacije v finančnem sektorju morajo zagotoviti varnostno kopiranje kot del ukrepov za neprekinjenost IKT.

11.7 COBIT 2019

11.7.1 BAI04.05: zahteva dokumentirane strategije varnostnega kopiranja.

11.7.2 DSS04.07: poudarja redno testiranje in kontrolo procesov varnostnega kopiranja ter obnove podatkov.