					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P15S					Naziv dokumenta: **Politika sigurnosnog kopiranja i oporavka**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađeno sa standardima i propisima

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 8	Kontrole sigurnosnog kopiranja u skladu sa zahtjevima ISMS-a
ISO/IEC 27002:2022	Kontrole 5.29, 8	Najbolje prakse za sigurnosno kopiranje i integraciju s kontinuitetom poslovanja
NIST SP 800-53 Rev.5	CP-9, MP-6	Sigurnosne kopije i zaštita medija
EU NIS2	Članak 21(2)(c)	Otpornost i kontinuitet kroz sigurnosne kopije
EU DORA	Članak 10(1)	Kontinuitet IKT-a – sigurnosne kopije za financijske organizacije
COBIT 2019	BAI04.05, DSS04	Dokumentiranje i testiranje sigurnosnih kopija te kontrola procesa
EU GDPR	Članci 5(1)(f), 32(1)(c)	Cjelovitost, dostupnost i pravodobna obnova podataka

1. Svrha

1.1 Ova politika definira način na koji organizacija provodi i upravlja sigurnosnim kopiranjem radi osiguravanja kontinuiteta poslovanja, zaštite od gubitka podataka i pravodobnog oporavka nakon incidenata.

1.2 Uspostavlja obvezujuća pravila za izradu, pohranu i obnovu sigurnosnih kopija sustava i podataka, osobito u SME okruženjima bez složene IT infrastrukture.

1.3 Ova politika podupire spremnost za reviziju i certifikaciju prema normi ISO/IEC 27001 osiguravajući da su ključne kontrole sigurnosnog kopiranja uspostavljene, dosljedno primijenjene i redovito preispitivane.

1.4 Sposobnost organizacije za oporavak od tehničkih kvarova, slučajnog brisanja ili kibernetičkih incidenata ovisi o strogom pridržavanju ove politike.

2. Opseg

2.1 Ova politika primjenjuje se na sve poslovne sustave i podatke, uključujući:

2.1.1 financijske evidencije, podatke o klijentima i kadrovske podatke

2.1.2 stolna računala, prijenosna računala, poslužitelje i aplikacije u oblaku koje se koriste u poslovnim procesima

2.1.3 medije za sigurnosne kopije, kao što su USB uređaji, vanjska pohrana ili sigurnosne kopije u uslugama u oblaku

2.2 Također se primjenjuje na sve osobe odgovorne za rukovanje sigurnosnim kopijama ili upravljanje postupcima sigurnosnog kopiranja, uključujući:

2.2.1 glavnog rukovoditelja (GM) ili drugu imenovanu odgovornu osobu

2.2.2 vanjske pružatelje IT podrške ili konzultante

2.2.3 sve zaposlenike odgovorne za pohranu podataka na odobrenim lokacijama

3. Ciljevi

3.1 Osigurati da se svi poslovno kritični podaci i sustavi sigurnosno kopiraju u primjerenim intervalima, na temelju procjene rizika i operativnih potreba.

3.2 Osigurati da se podaci mogu oporaviti pravodobno i cjelovito nakon prekida rada.

3.3 Spriječiti neovlašten pristup, neovlaštenu izmjenu ili gubitak podataka iz sigurnosnih kopija primjenom odgovarajućih kontrola pohrane.

3.4 Jasno dodijeliti uloge i odgovornosti za provedbu i testiranje postupaka sigurnosnog kopiranja i oporavka te osigurati njihovo izvršavanje.

3.5 Poduprijeti usklađenost s normom ISO/IEC 27001, GDPR-om i drugim regulatornim obvezama putem strukturiranih i dokumentiranih praksi sigurnosnog kopiranja.

4. Uloge i odgovornosti

4.1 Glavni rukovoditelj (GM)

4.1.1 Odobrava ovu politiku i osigurava njezinu provedbu

4.1.2 Dodjeljuje resurse i utvrđuje odgovornost za aktivnosti sigurnosnog kopiranja i oporavka

4.1.3 Preispituje neuspjela sigurnosna kopiranja, incidente i odstupanja od politike

4.1.4 Provodi godišnje preglede politike i osigurava spremnost za reviziju

4.2 Vanjski pružatelj IT podrške (ako je primjenjivo)

4.2.1 Uspostavlja i upravlja rješenjima za sigurnosno kopiranje (lokalnim ili u oblaku)

4.2.2 Prati uspješnost sigurnosnih kopija i planira testove oporavka

4.2.3 Neuspjehe i incidente izravno prijavljuje GM-u

4.2.4 Osigurava šifriranje, ograničenje pristupa i pravilno rukovanje medijima za sigurnosne kopije

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Zahtjevi za pregled i ažuriranje

9.1 Ovu politiku GM mora pregledati najmanje jednom godišnje. Okidači za izvanredni pregled uključuju:

9.1.1 značajne promjene u sustavima ili metodama pohrane

9.1.2 uvođenje novih platformi u oblaku ili IT platformi

9.1.3 pravne ili regulatorne promjene koje utječu na oporavak podataka

9.1.4 nalaze revizije ili incidente

9.2 GM je odgovoran za pokretanje pregleda, odobravanje izmjena i priopćavanje ažuriranja.

9.3 Verzije politike moraju se pratiti i arhivirati. Zamijenjene verzije moraju imati ograničen pristup kako bi se izbjegla zabuna tijekom revizija ili aktivnosti oporavka poslovanja.

10. Povezane politike i poveznice

10.1 Ova je politika usklađena sa sljedećim SME politikama i ovisi o njima:

10.1.1 P14S – Politika zadržavanja podataka i zbrinjavanja: definira koliko dugo se podaci iz sigurnosnih kopija moraju čuvati i kako se sigurno brišu.

10.1.2 P13S – Politika klasifikacije i označavanja podataka: pomaže odrediti prioritet podataka koji se moraju sigurnosno kopirati na temelju razina klasifikacije.

10.1.3 P30S – Politika odgovora na incidente: obuhvaća postupke kada sigurnosne kopije ne uspiju ili kada je potreban oporavak podataka nakon povrede ili prekida rada.

10.1.4 P2S – Politika uloga i odgovornosti u upravljanju: dodjeljuje jasne ovlasti za nadzor sigurnosnog kopiranja i provedbu politike.

10.1.5 P17S – Politika zaštite podataka i privatnosti: osigurava da je postupanje s osobnim podacima u sigurnosnim kopijama usklađeno s pravnim zahtjevima i pravilima privatnosti.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 8.1: operativno planiranje i kontrola sigurnosnog kopiranja kao dijela ISMS-a

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.13: propisuje najbolje prakse za raspoređivanje sigurnosnih kopija, praćenje i obnovu

11.2.2 Dodatak A, Kontrola 5.29: integracija sigurnosnih kopija s kontinuitetom poslovanja i spremnošću za oporavak

11.3 NIST SP 800-53 Rev.

11.3.1 CP-9 (planiranje kontinuiteta): definira strukturirane strategije sigurnosnog kopiranja za poslovnu otpornost

11.3.2 MP-6 (zaštita medija): zahtijeva sigurno rukovanje medijima za sigurnosne kopije i njihovo uništavanje

11.4 EU GDPR

11.4.1 Članak 5(1)(f): propisuje cjelovitost i dostupnost osobnih podataka

11.4.2 Članak 32(1)(c): zahtijeva mogućnost pravodobne obnove pristupa osobnim podacima

11.5 Direktiva EU NIS2

11.5.1 Članak 21(2)(c): zahtijeva sigurnosne kopije i oporavak kao dio planiranja otpornosti i kontinuiteta

11.6 EU DORA

11.6.1 Članak 10(1): organizacije u financijskom sektoru moraju osigurati sigurnosne kopije kao dio mjera kontinuiteta IKT-a

11.7 COBIT 2019

11.7.1 BAI04.05: zahtijeva dokumentirane strategije sigurnosnog kopiranja

11.7.2 DSS04.07: naglašava redovito testiranje i kontrolu nad postupcima sigurnosnog kopiranja i oporavka podataka