					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P15					Naziv dokumenta: **Politika sigurnosnog kopiranja i vraćanja podataka**							
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 regulativom

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točke 6.1.3, 8.	Obrada rizika, planiranje i operativne kontrole sigurnosnog kopiranja
ISO/IEC 27002:2022	Kontrole 8.13, 5.28, 5.	Upravljanje sigurnosnim kopijama, sigurno zbrinjavanje
NIST SP 800-53 Rev.5	CP-9, CP-10, SI-12, MP-6	Zahtjevi za sigurnosno kopiranje sustava, oporavak i sanitizaciju medija
GDPR EU	Članak 32, uvodna izjava 49	Vraćanje i dostupnost osobnih podataka, kontinuitet poslovanja
Direktiva NIS2 EU	Članak 21(2)(c-e)	Kontrole sigurnosnog kopiranja i kontinuiteta radi otpornosti
Uredba DORA EU	Članci 10, 11	Zahtjevi financijskog sektora za sigurnosno kopiranje, oporavak i testiranje
COBIT 2019	DSS01, DSS04, MEA	Operacije sigurnosnog kopiranja, kontinuitet i praćenje usklađenosti

1. Svrha

1.1 Svrha ove politike jest utvrditi obvezne zahtjeve za sigurnosno kopiranje i vraćanje podataka, sustava i aplikacija radi potpore operativnoj otpornosti, cjelovitosti podataka i kontinuitetu poslovanja.

1.2 Ova politika uspostavlja standardizirani okvir za:

1.2.1 zaštitu podataka organizacije od gubitka uslijed brisanja, oštećenja, otkaza ili kibernetičkih napada

1.2.2 definiranje očekivanja oporavka putem jasno utvrđenih parametara RTO-a (ciljno vrijeme oporavka) i RPO-a (ciljna točka oporavka)

1.2.3 integraciju operacija sigurnosnog kopiranja sa širim ISMS-om i planovima kontinuiteta poslovanja (BCP/DRP)

1.2.4 osiguravanje usklađenosti s primjenjivim zakonima i sektorskim propisima u pogledu dostupnosti i mogućnosti oporavka

1.3 Ova politika provodi kontrole norme ISO/IEC 27001:2022 povezane sa sigurnim zbrinjavanjem podataka (5.28), otpornošću (5.29) i operativnim oporavkom (8.13) te je usklađena s dobrim praksama iz norme ISO/IEC 27002:2022, okvira NIST SP 800-53 Rev.5, GDPR-a, DORA-e i NIS2.

2. Opseg

2.1 Ova politika primjenjuje se na:

2.1.1 sve poslovno kritične i operativne sustave unutar opsega ISMS-a

2.1.2 sve strukturirane i nestrukturirane poslovne podatke, uključujući baze podataka, datoteke, e-poštu i konfiguracije

2.1.3 sva okruženja — lokalna, oblačna, hibridna te udaljenu/izvanlokacijsku pohranu

2.1.4 svo osoblje odgovorno za upravljanje, izvršavanje, provjeru ili vraćanje procesa sigurnosnog kopiranja

2.2 Ova politika također se primjenjuje na:

2.2.1 medije i infrastrukturu za sigurnosno kopiranje, uključujući fizičke vrpce, virtualne uređaje, snimke diskova i rješenja za sigurnosno kopiranje temeljena na uslugama u oblaku

2.2.2 pružatelje usluga treće strane ugovorene za hosting, upravljanje ili obradu sigurnosnih kopija organizacije

2.2.3 sigurnosne kopije dnevničkih zapisa, konfiguracija, revizijskog traga i operativne dokumentacije ključne za kontinuitet

2.3 Sustavi izričito isključeni iz sigurnosnog kopiranja moraju biti dokumentirani, podvrgnuti procjeni rizika i formalno prihvaćeni od strane voditelja ISMS-a i vlasnika sustava.

3. Ciljevi

3.1 Osigurati da se za sve kritične sustave i podatke pouzdano izrađuju sigurnosne kopije uz dostatnu učestalost, redundantnost i sigurnosne kontrole.

3.2 Osigurati mehanizme vraćanja koji ispunjavaju definirana očekivanja RTO-a i RPO-a u skladu s procjenama utjecaja na poslovanje.

3.3 Održavati potpunu dokumentaciju postupaka sigurnosnog kopiranja, rasporeda zadržavanja, uloga i tehnologija.

3.4 Provjeravati djelotvornost operacija sigurnosnog kopiranja kroz sustavno testiranje vraćanja, evidentiranje neuspjeha i praćenje korektivnih radnji.

3.5 Štititi podatke iz sigurnosnih kopija od neovlaštenog pristupa, izmjene ili uništenja tijekom cijelog životnog ciklusa.

3.6 Omogućiti usklađenost sa:

3.6.1 zahtjevima norme ISO/IEC 27001 za operativne kontrole i kontrole kontinuiteta

3.6.2 obiteljima kontrola NIST SP 800-53 CP i MP za sigurnosno kopiranje i sanitizaciju

3.6.3 člankom 32. GDPR-a i uvodnom izjavom 49 za vraćanje pristupa osobnim podacima

3.6.4 člankom 10. Uredbe DORA EU i člankom 21. Direktive NIS2 EU za kontinuitet IKT-a i otpornost

3.7 Osigurati da usluge sigurnosnog kopiranja koje pruža treća strana ispunjavaju ugovorne i regulatorne sigurnosne obveze, uključujući šifriranje, zbrinjavanje i protokole obavješćivanja.

4. Uloge i odgovornosti

4.1 Izvršno rukovodstvo

4.1.1 Odobrava ovu politiku i osigurava da su poslovno kritični sustavi primjereno zaštićeni odobrenim praksama sigurnosnog kopiranja i vraćanja podataka.

4.1.2 Odgovorno je za osiguravanje odgovarajućih resursa za operacije sigurnosnog kopiranja i njihov periodični pregled radi usklađenosti s regulatornim zahtjevima.

4.2 Glavni direktor za informacijsku sigurnost (CISO)

4.2.1 Vlasnik je ove politike i osigurava njezinu usklađenost sa širim okvirima informacijske sigurnosti, upravljanja rizicima i kontinuiteta poslovanja.

4.2.2 Nadzire integraciju postupaka sigurnosnog kopiranja u BCP/DRP, odgovor na incidente i planiranje otpornosti.

4.2.3 Pregledava iznimke povezane sa sigurnosnim kopiranjem i procjenjuje prijedloge za prihvaćanje rizika u slučaju isključenja kritičnih sustava.

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

9. Zahtjevi za pregled i ažuriranje

9.1 Ova politika mora se pregledavati najmanje jednom godišnje ili ranije ako to uzrokuju:

9.1.1 promjene strategije kontinuiteta poslovanja ili oporavka od katastrofe

9.1.2 nove regulatorne ili zakonske obveze koje utječu na učestalost sigurnosnog kopiranja ili zadržavanje podataka

9.1.3 promjene arhitekture sustava, alata za sigurnosno kopiranje ili pružatelja usluga

9.1.4 značajni incidenti ili nalazi revizije povezani s gubitkom podataka ili neuspjehom oporavka

9.2 Pregled koordinira CISO u suradnji sa:

9.2.1 timom za IT infrastrukturu i operacije

9.2.2 unutarnjom revizijom

9.2.3 službenikom za zaštitu podataka (DPO)

9.2.4 timovima za kontinuitet poslovanja i oporavak od katastrofe

9.3 Rasporedi sigurnosnog kopiranja, popisi uključenih sustava, dokumentacija vraćanja i dnevnici iznimaka moraju se pregledavati usporedno kako bi se osiguralo:

9.3.1 točnost obuhvata sigurnosnog kopiranja za svu kritičnu imovinu

9.3.2 usklađenost sa zahtjevima RTO-a/RPO-a i zadržavanja

9.3.3 potpunost dnevnika testiranja i izvješća o incidentima

9.3.4 otklanjanje prethodno utvrđenih nedostataka u kontrolama

9.4 Sva ažuriranja moraju:

9.4.1 biti pod verzijskom kontrolom i zadržana u repozitoriju dokumenata ISMS-a

9.4.2 uključivati sažetak promjena i obrazloženje

9.4.3 biti odobrena od strane izvršnog rukovodstva

9.4.4 biti priopćena svom pogođenom tehničkom i poslovnom osoblju

10. Povezane politike i poveznice

10.1 Ova politika izravno podupire i povezana je sa sljedećim dokumentima:

10.1.1 P6 - Politika upravljanja rizicima: Utvrđuje prioritizaciju zaštite sigurnosnog kopiranja za sustave i usluge temeljenu na riziku.

10.1.2 P12 - Politika upravljanja imovinom: Osigurava da su sustavi obuhvaćeni sigurnosnim kopiranjem evidentirani u popisu imovine i povezani s praćenjem životnog ciklusa i klasifikacijom.

10.1.3 P13 - Politika klasifikacije i označavanja podataka: Utvrđuje koje kategorije podataka zahtijevaju sigurnosno kopiranje, uključujući označavanje metapodataka radi određivanja prioriteta.

10.1.4 P14 - Politika zadržavanja i zbrinjavanja podataka: Usklađuje zadržavanje sigurnosnih kopija s regulatornim ograničenjima zadržavanja i pravilnim zbrinjavanjem medija kojima je istekao rok uporabe.

10.1.5 P16 - Politika maskiranja podataka i pseudonimizacije: Podupire minimizaciju podataka tijekom sigurnosnog kopiranja osjetljivih skupova podataka.

10.1.6 P30 - Politika odgovora na incidente: Aktivira se u slučaju neuspjeha sigurnosnog kopiranja, problema s vraćanjem ili kompromitacije repozitorija podataka sigurnosnih kopija.

10.2 Ove međusobno povezane politike čine koherentan okvir kojim se osigurava da je upravljanje sigurnosnim kopiranjem ugrađeno u širi ISMS organizacije i strategiju operativne otpornosti.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001:

11.1.1 Točka 6.1.3 - Plan obrade rizika: Podupire prioritizaciju sigurnosnog kopiranja i planiranje vraćanja temeljene na riziku.

11.1.2 Točka 8.1 - Operativno planiranje i kontrola: Integrira kontrole oporavka i kontinuiteta kao dio operativnih zaštitnih mjera.

11.1.3 Kontrola Priloga A 5.28 - Sigurno zbrinjavanje ili ponovna uporaba opreme: Obuhvaća sigurnu sanitizaciju medija sigurnosnih kopija.

11.1.4 Kontrola Priloga A 5.29 - Informacijska sigurnost tijekom poremećaja: Osigurava mogućnosti vraćanja tijekom incidenata ili katastrofa.

11.1.5 Kontrola Priloga A 8.13 - Sigurnosno kopiranje informacija: Izravno se provodi kroz planirane, testirane i sigurne operacije sigurnosnog kopiranja.

11.2 ISO/IEC 27002:2022 - Kontrole 8.13, 5.28, 5.: Ove kontrole dodatno potvrđuju zahtjev za redovitim sigurnosnim kopijama, provjerom cjelovitosti i planiranjem vraćanja u svim IT okruženjima.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-9 - Sigurnosno kopiranje sustava: Uspostavlja sveobuhvatne postupke sigurnosnog kopiranja, uključujući pohranu izvan lokacije i testiranje vraćanja.

11.3.2 CP-10 - Oporavak i vraćanje sustava: Zahtijeva provjerene postupke za potpuno ili djelomično vraćanje usklađeno s ciljevima oporavka.

11.3.3 MP-6 - Sanitizacija medija: Osigurava sigurno postupanje sa zastarjelim medijima sigurnosnih kopija.

11.3.4 SI-12 - Postupci postupanja s informacijama: Dodatno potvrđuje odgovornosti za sigurnosno kopiranje i oporavak osjetljivih podataka.

11.4 GDPR EU (2016/679):

11.4.1 Članak 32 - Sigurnost obrade: Propisuje mogućnosti vraćanja i zaštitne mjere dostupnosti podataka, posebno za osobne podatke.

11.4.2 Uvodna izjava 49: Podupire mjere kontinuiteta poslovanja i oporavka od katastrofe, uključujući sigurno sigurnosno kopiranje kao dio otpornosti organizacije.

11.5 Direktiva NIS2 EU (2022/2555):

11.5.1 Članak 21(2)(c-e): Zahtijeva tehničke i organizacijske mjere, uključujući kontrole sigurnosnog kopiranja i kontinuiteta, radi osiguravanja otpornosti usluga.

11.6 Uredba DORA EU (2022/2554):

11.6.1 Članak 10 - Kontinuitet poslovanja IKT-a: Zahtijeva da financijski subjekti imaju potpuno sigurnosno kopiranje podataka, oporavak i planiranje kontinuiteta.

11.6.2 Članak 11 - Testiranje planova kontinuiteta poslovanja IKT-a: Naglašava provjeru sposobnosti oporavka putem redovitog testiranja.

11.7 COBIT 2019:

11.7.1 DSS01 - Upravljane operacije: Podupire pouzdanu isporuku usluga kroz zaštićenu dostupnost podataka.

11.7.2 DSS04 - Upravljani kontinuitet: Definira strateške i operativne kontrole kontinuiteta, uključujući provjerene sigurnosne kopije.

11.7.3 MEA03 - Praćenje, vrednovanje i procjena usklađenosti: Zahtijeva periodični pregled mjera kontinuiteta, uključujući djelotvornost kontrola sigurnosnog kopiranja.