					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P05					Naziv dokumenta: **Politika upravljanja promjenama**							
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**

Pravna napomena (autorska prava i ograničenja uporabe)

(C) 2025 Clarysec LLC. All rights reserved.

Ovaj dokument intelektualno je vlasništvo društva Clarysec LLC. Nijedan dio ovog dokumenta ne smije se kopirati, ponovno upotrebljavati, distribuirati niti mijenjati u komercijalne svrhe ili svrhe implementacije bez izričitog prethodnog pisanog odobrenja.

Neovlaštena uporaba strogo je zabranjena i može rezultirati pravnim postupkom.

Za licenciranje kontaktirajte: info@clarysec.com

Usklađeno sa standardima i regulativom

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točke 6.1, 5.15	Obuhvaća postupanje s rizicima, kontrolu pristupa i upravljanje promjenama
ISO/IEC 27002:2022	Kontrola 8	Propisuje strukturirani postupak upravljanja promjenama
NIST SP 800-53 Rev.5	CM-2 do CM-14	Kontrole upravljanja konfiguracijom
GDPR EU	Članci 32(1)(b–d), 25; uvodna izjava 78	Tehničke i organizacijske mjere za sigurnost sustava i podataka tijekom promjena
Direktiva EU NIS2	Članak 21(2)(a, b, d, e)	Propisuje upravljanje rizicima ICT promjena
Uredba EU DORA	Članci 5, 8, 12	Uređuje operativni i ICT rizik te prijavljivanje incidenata
COBIT 2019	BAI06, BAI02, BAI03, DSS01, MEA01, MEA03	Strukturirani zahtjevi za upravljanje IT promjenama, uspješnost i usklađenost

1. Svrha

1.1. Ova politika uspostavlja formalni okvir za pokretanje, procjenu, odobravanje, provedbu i pregled promjena u informacijskim sustavima, infrastrukturi, aplikacijama i povezanim procesima organizacije.

1.2. Njome se osigurava da se sve promjene provode na kontroliran i revizijski dokaziv način, uz smanjenje rizika od prekida rada, narušavanja sigurnosti ili neusklađenosti s regulatornim zahtjevima.

1.3. Podržava kontrolu 8.32 Dodatka A norme ISO/IEC 27001:2022 provedbom sigurnih, dokumentiranih i s rizikom usklađenih praksi upravljanja promjenama.

1.4. Ova politika također osigurava sljedivost odluka o promjenama i promiče operativnu otpornost tijekom planiranih ili hitnih izmjena.

2. Opseg

2.1. Ova politika primjenjuje se na sve promjene koje utječu na sustave, podatke i okruženja unutar opsega ISMS-a, uključujući:

2.1.1. IT infrastrukturu (u vlastitim prostorijama, u oblaku, hibridno)

2.1.2. produkcijska, pretprodukcijska i okruženja za oporavak od katastrofe

2.1.3. poslovne aplikacije, API-je i integracije

2.1.4. konfiguracijske postavke, zakrpe, izdanja softvera i migracije sustava

2.1.5. hitne ispravke te projektne ili planirane promjene

2.2. Ova politika uređuje promjene koje pokreću:

2.2.1. interni zaposlenici (IT operacije, razvojni inženjeri, vlasnici sustava)

2.2.2. vanjski dobavljači, pružatelji upravljanih usluga (MSP) i ugovorni izvođači

2.2.3. projektni timovi tijekom implementacije sustava, nadogradnji ili tranzicije usluga

2.3. Ova politika ne primjenjuje se na:

2.3.1. privremena testna ili razvojna okruženja bez pristupa produkcijskim podacima

2.3.2. osobne korisničke konfiguracije (obuhvaćene Politikom prihvatljive uporabe)

2.3.3. promjene na sustavima izvan granica kontrole organizacije, osim ako utječu na integriranu imovinu ili obveze usklađenosti

3. Ciljevi

3.1. Osigurati da se sve promjene pregledaju, odobre, testiraju i dokumentiraju prije provedbe.

3.2. Održavati dostupnost sustava, cjelovitost podataka i kontinuitet usluga tijekom i nakon provedbe promjene.

3.3. Zahtijevati definirane klasifikacije promjena, planove povrata i procjene rizika za sve vrste promjena.

3.4. Omogućiti transparentno odlučivanje i eskalaciju kroz strukturirano upravljanje.

3.5. Podržati spremnost za reviziju kroz sljedive zapise o promjenama i postimplementacijske preglede.

3.6. Osigurati razdvajanje dužnosti i smanjiti rizik od neovlaštenih ili sukobljenih promjena u kritičnim sustavima.

4. Uloge i odgovornosti

4.1. Izvršni menadžment

4.1.1. Odobrava Politiku upravljanja promjenama i osigurava njezinu usklađenost sa strateškim ciljevima i regulatornim obvezama.

4.1.2. Odobrava programe promjena s velikim utjecajem ili međufunkcionalne programe promjena u okviru nadzora upravljanja.

4.1.3. Osigurava potrebne resurse i proračun za alate za kontrolu promjena i osposobljavanje osoblja.

4.2. Savjetodavni odbor za promjene

4.2.1. Pregledava i odobrava standardne i velike promjene te osigurava odgovarajuću procjenu rizika, utjecaja i međuovisnosti.

4.2.2. Provjerava planove povrata, rezultate testiranja, komunikaciju s dionicima i raspored provedbe.

4.2.3. Sastoji se od vlasnika sustava, predstavnika informacijske sigurnosti, IT operacija, poslovnih predstavnika i predstavnika usklađenosti.

4.2.4. Može delegirati odluke za niskorizične ili hitne promjene pod dokumentiranim uvjetima.

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

9. Zahtjevi za pregled i ažuriranje

9.1. Pokretači pregleda i učestalost

9.1.1. Ova politika mora se pregledati jednom godišnje ili nakon:

9.1.1.1. velikih promjena u IT-u ili infrastrukturi

9.1.1.2. značajnih incidenata povezanih s neuspjelim ili neovlaštenim promjenama

9.1.1.3. regulatornih ažuriranja ili novih pravnih obveza povezanih s promjenama

9.1.1.4. implementacije novih alata ili CMS platformi

9.2. Postupak pregleda Politike upravljanja promjenama

9.2.1. Voditelj promjena vodi postupak pregleda u suradnji s:

9.2.1.1. IT-om, sigurnošću i operacijama

9.2.1.2. unutarnjom revizijom, funkcijom praćenja usklađenosti i upravljanjem rizicima

9.2.1.3. predstavnicima CAB-a

9.2.2. Ažuriranja moraju pregledati i odobriti Izvršni menadžment i Upravljački odbor ISMS-a.

9.2.3. Ponovno izdane verzije moraju se evidentirati u registru dokumenata i priopćiti zahvaćenim stranama uz ponovno potvrđivanje upoznatosti, prema potrebi.

9.3. Upravljanje dokumentom i verzijama

9.3.1. Sve verzije moraju sadržavati:

9.3.1.1. identifikator politike, naziv i razinu klasifikacije

9.3.1.2. vlasnika i povijest izmjena

9.3.1.3. zapisnik promjena i datum stupanja na snagu

9.3.1.4. tijelo nadležno za odobrenje

9.3.2. Arhivirane verzije moraju se čuvati u skladu s Politikom zadržavanja dokumenata (najmanje 3 godine).

10. Povezane politike i poveznice

10.1. Ova politika izravno je povezana sa sljedećim politikama i podupire njihovu primjenu:

10.1.1. P1 – Politika informacijske sigurnosti: Uspostavlja zahtjev za formalnim sigurnosnim kontrolama i odgovornošću na razini procesa, uključujući upravljanje promjenama.

10.1.2. P2 – Politika uloga i odgovornosti u upravljanju: Definira ovlasti za odobravanje i razdvajanje dužnosti relevantne za odobravanje i nadzor promjena.

10.1.3. P4 – Politika kontrole pristupa: Osigurava da prava pristupa osoba koje provode i pregledavaju promjene slijede načelo najmanjih privilegija.

10.1.4. P6 – Politika upravljanja rizicima: Osigurava da sve promjene podliježu odgovarajućem vrednovanju rizika i strategijama ublažavanja.

10.1.5. P33 – Politika praćenja revizije i usklađenosti: Uređuje provjeru i revizijski pregled zapisa o upravljanju promjenama i kršenja.

10.2. Ove politike zajedno omogućuju dokaziv, sljediv i siguran životni ciklus upravljanja promjenama unutar okvira ISMS-a.

11. Referentni standardi i okviri

11.1. ISO/IEC 27001:2022

11.1.1. Točka 6.1 – Radnje za postupanje s rizicima i prilikama: Ova politika podupire identifikaciju, vrednovanje i kontrolu rizika povezanih s promjenama.

11.1.2. Točka 5.15 – Kontrola pristupa: Osigurava da je pristup tijekom promjena kontroliran i sljediv.

11.1.3. Kontrola 8.32 Dodatka A – Upravljanje promjenama: Ova politika u cijelosti provodi zahtjev za upravljanjem promjenama na sredstvima za obradu informacija i sustavima na planiran i kontroliran način.

11.2. ISO/IEC 27002:2022 – Kontrola 8

11.2.1. Jača provedbu strukturiranog postupka upravljanja promjenama, uključujući klasifikaciju promjena, odobravanje, testiranje, povrat i dokumentaciju.

11.3. NIST SP 800-53 Rev.5

11.3.1. Obitelj CM (CM-1 do CM-14): Ova politika usko je usklađena s kontrolama upravljanja konfiguracijom, uključujući početne konfiguracije (CM-2), kontrolu promjena konfiguracije (CM-3), analizu sigurnosnog utjecaja (CM-4) i ograničenja pristupa (CM-5).

11.3.2. Obitelj AU (AU-2, AU-6, AU-12): Mehanizmi bilježenja i revizije navedeni u ovoj politici podupiru sljedivost događaja i pregled usklađenosti za aktivnosti povezane s promjenama.

11.3.3. RA-3, RA-5: Procjene rizika potaknute promjenama i skeniranja ranjivosti ugrađeni su u postupak vrednovanja promjena.

11.3.4. PM-11 (Definicija misije/poslovnog procesa): Osigurava da se kontinuitet poslovanja i operativni ciljevi očuvaju tijekom promjena.

11.4. GDPR EU (2016/679)

11.4.1. Članak 32(1)(b–d): Ova politika podupire zahtjev za odgovarajućim tehničkim i organizacijskim mjerama za osiguranje sigurnosti podataka, posebno tijekom promjena sustava.

11.4.2. Članak 25 – Zaštita podataka ugrađena u dizajn i prema zadanim postavkama: Osigurava da promjene koje utječu na osobne podatke integriraju privatnost i sigurnost u dizajn i uvođenje.

11.4.3. Uvodna izjava 78: Zahtijeva da voditelji obrade uspostave mehanizme, kao što su politike kontrole promjena, radi osiguravanja trajne povjerljivosti, cjelovitosti i otpornosti sustava obrade.

11.5. Direktiva EU NIS2 (2022/2555)

11.5.1. Članak 21(2)(a, b, d, e): Propisuje tehničke i organizacijske mjere za upravljanje ICT rizicima, uključujući one koji proizlaze iz promjena sustava, ažuriranja softvera i izmjena infrastrukture.

11.6. Uredba EU DORA (2022/2554)

11.6.1. Članak 5 – Okvir upravljanja i unutarnjih kontrola: Ova politika provodi načela upravljanja operativnim rizikom povezana s ICT promjenama i ažuriranjima.

11.6.2. Članak 8 – Okvir za upravljanje ICT rizicima: Propisuje da financijski subjekti upravljaju svim promjenama koje utječu na ICT sustave kroz strukturirane postupke upravljanja promjenama, što se u ovoj politici odražava kroz zahtjeve za klasifikaciju, testiranje, povrat i dokumentaciju.

11.6.3. Članak 12 – Prijavljivanje incidenata: Osigurava da su neuspjele promjene koje dovode do ICT poremećaja sljedive, dokumentirane i prijavljene kada je primjenjivo.

11.7. COBIT 2019

11.7.1. BAI06 – Upravljane IT promjene: Ova politika izravno ispunjava ciljeve BAI06 uspostavom strukturiranih tijekova rada za odobravanje promjena, procjenu utjecaja, komunikaciju i testiranje.

11.7.2. BAI02 – Upravljana definicija zahtjeva i BAI03 – Upravljana identifikacija i izgradnja rješenja: Osiguravaju da se poslovno vođene promjene pregledavaju i provode na siguran način.

11.7.3. DSS01 – Upravljane operacije: Podupire trajnu cjelovitost sustava tijekom provedbe promjena.

11.7.4. MEA01 i MEA03 – Praćenje, vrednovanje i procjena uspješnosti i usklađenosti: Omogućuju kontinuirani nadzor djelotvornosti i provedbe politike upravljanja promjenama.