					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P05S					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**

Usklađenost sa standardima i regulativom

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 6.1, 8.	
ISO/IEC 27002:2022	Kontrola 8.	
NIST SP 800-53 Rev.5	CM-2 do CM-5, CM-11	
Direktiva EU NIS2	Članak 21(2)(b)	
Uredba EU DORA	Članci 6(9), 8(4)(b)	
COBIT 2019	BAI06, DSS	

1. Svrha

1.1 Ovom se politikom osigurava da su sve promjene na IT sustavima, konfiguracijama, poslovnim aplikacijama i uslugama u oblaku planirane, procijenjene s aspekta rizika, testirane i odobrene prije provedbe.

1.2 Cilj je smanjiti operativne poremećaje, sigurnosne rizike i prekide usluge uspostavom pojednostavljenog, ali obvezujućeg procesa koji se primjenjuje i u malim organizacijama s ograničenim resursima.

1.3 Ova politika podupire certifikaciju prema normi ISO/IEC 27001:2022 formaliziranjem načina upravljanja i dokumentiranja tehničkih i operativnih promjena.

2. Područje primjene

2.1 Ova se politika primjenjuje na:

2.1.1 zaposlenike i rukovoditelje odjela koji predlažu ili provode promjene

2.1.2 vanjske pružatelje IT usluga koji upravljaju sustavima ili softverom

2.1.3 glavnog direktora, koji snosi ukupnu odgovornost za odobravanje promjena

2.2 Obuhvaća promjene koje se odnose na:

2.2.1 softver (ažuriranja, zakrpe, nove aplikacije)

2.2.2 hardver (zamjene, nadogradnje)

2.2.3 mrežne konfiguracije i konfiguracije vatrozida

2.2.4 usluge u oblaku, prava pristupa korisnika ili integracije s dobavljačima

2.2.5 promjene kritičnih poslovnih procesa koje uključuju informacijske sustave

2.3 Planirane i hitne promjene ulaze u područje primjene ove politike.

3. Ciljevi

3.1 Osigurati da su sve promjene u IT-u i poslovnim sustavima odobrene, dokumentirane i da ih je moguće vratiti u prethodno stanje u slučaju problema.

3.2 Spriječiti neplanirane zastoje, gubitak podataka i sigurnosne incidente uzrokovane nekontroliranim promjenama.

3.3 Definirati jednostavne i ponovljive postupke za podnošenje, odobravanje, testiranje i povrat promjena.

3.4 Održavati dokaziv zapisnik promjena koji podupire operativnu odgovornost i usklađenost s regulatornim zahtjevima.

3.5 Omogućiti odlučivanje temeljeno na riziku za značajne ili osjetljive promjene.

4. Uloge i odgovornosti

4.1 Glavni direktor

4.1.1 Snosi krajnju odgovornost za sve veće promjene.

4.1.2 Pregledava i odobrava nerutinske, kritične ili visokorizične promjene.

4.1.3 Tromjesečno ili nakon većih incidenata pregledava zapisnik promjena.

4.2 IT podrška ili vanjski pružatelj IT usluga

4.2.1 Provodi promjene, uključujući promjene konfiguracije, zakrpavanje i migracije sustava.

4.2.2 Održava osnovni zapisnik promjena s datumima, vrstama promjena, ishodima i odobravateljima.

4.2.3 Testira promjene prije provedbe i prema potrebi primjenjuje postupke povrata.

4.2.4 Obavještava zahvaćene korisnike prije i nakon većih promjena.

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

9. Zahtjevi za pregled i ažuriranje

9.1 Godišnji pregled

9.1.1 Ovu politiku mora jednom godišnje pregledati glavni direktor ili imenovani IT kontakt kako bi se osigurala usklađenost s trenutačnim sustavima, procesima rada i regulatornim zahtjevima.

9.2 Izvanredni pregledi

9.2.1 Pregledi se moraju pokrenuti i u sljedećim slučajevima:

9.2.1.1 sigurnosni incidenti uzrokovani neodgovarajućim postupanjem s promjenama

9.2.1.2 uvođenje novih IT sustava

9.2.1.3 promjene relevantnih standarda kao što su ISO, NIS2 ili DORA

9.3 Dokumentiranje ažuriranja

9.3.1 Promjene ove politike moraju biti pod kontrolom verzija i odobrene od strane glavnog direktora. Svaka verzija mora sadržavati datum, sažetak promjena i odobravatelja.

9.4 Komunikacija politike

9.4.1 Sva ažuriranja moraju se priopćiti svim zahvaćenim zaposlenicima i vanjskim pružateljima. Dokumentacija mora biti ažurirana na svim relevantnim mjestima pohrane i upućivanja (npr. portal za zaposlenike, dijeljeni diskovi).

10. Povezane politike i poveznice

10.1 Ova je politika usko povezana sa sljedećim SME politikama:

10.1.1 P2S – Politika upravljačkih uloga i odgovornosti: definira ovlasti za odobravanje promjena.

10.1.2 P4S – Politika kontrole pristupa: osigurava da se izmjene pristupa koje proizlaze iz promjena pravilno dokumentiraju i provedu.

10.1.3 P7S – Politika uvođenja u posao i prestanka radnog odnosa: koordinira promjene povezane s prijelazima uloga i dodjelom prava pristupa.

10.1.4 P15S – Politika sigurnosnog kopiranja i obnove: osigurava da se koraci povrata i oporavka mogu provesti ako promjena ne uspije.

10.1.5 P30S – Politika odgovora na incidente: uređuje način postupanja s neuspjelim ili neovlaštenim promjenama kao sigurnosnim incidentima.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 6.1 – Planiranje temeljeno na riziku mora uključivati aktivnosti promjena.

11.1.2 Točka 8.1 – Operativne kontrole moraju se dosljedno primjenjivati na aktivnosti povezane s promjenama kako bi se osigurala cjelovitost usluge.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.32 – Pruža smjernice za sigurne procese upravljanja promjenama, uključujući dokumentiranje, testiranje i odobravanje.

11.3 NIST SP 800-53 Rev.

11.3.1 CM-2 – Osnovna konfiguracija sustava prije promjene.

11.3.2 CM-3 – Kontrola promjena konfiguracije.

11.3.3 CM-4 – Analiza utjecaja na sigurnost.

11.3.4 CM-5 – Odobravanje i dokumentiranje promjena.

11.3.5 CM-11 – Revizija i praćenje promjena.

11.4 Direktiva EU NIS2

11.4.1 Članak 21(2)(b) – Zahtijeva formalne postupke za tehničke i organizacijske sigurnosne mjere, uključujući upravljanje promjenama.

11.5 Uredba EU DORA

11.5.1 Članci 6(9) i 8(4)(b) – Zahtijevaju da financijski subjekti održavaju upravljanje promjenama i konfiguracijom za IKT sustave.

11.6 COBIT 2019

11.6.1 BAI06 – Upravljanje promjenama: naglašava planiranje, vrednovanje rizika i mogućnosti povrata.

11.6.2 DSS01 – Upravljanje operacijama: osigurava operativnu cjelovitost tijekom tehničkih prijelaza i promjena.