					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P05S					Naslov dokumenta: **Politika upravljanja sprememb**							
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**

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
ISO/IEC 27001:2022	Klavzula 6.1, 8	
ISO/IEC 27002:2022	Kontrola 8	
NIST SP 800-53 Rev. 5	CM-2 do CM-5, CM-11	
EU NIS2	Člen 21(2)(b)	
EU DORA	Člena 6(9), 8(4)(b)	
COBIT 2019	BAI06, DSS	

1. Namen

1.1 Ta politika zagotavlja, da so vse spremembe IT-sistemov, konfiguracij, poslovnih aplikacij ali storitev v oblaku načrtovane, ocenjene z vidika tveganj, testirane in odobrene pred izvedbo.

1.2 Namen te politike je z vzpostavitvijo poenostavljenega, vendar izvršljivega procesa zmanjšati operativne motnje, varnostna tveganja in izpade storitev, pri čemer se uporablja tudi v malih podjetjih z omejenimi viri.

1.3 Ta politika podpira certificiranje po standardu ISO/IEC 27001:2022 s formalizacijo načina upravljanja in dokumentiranja tehničnih ter operativnih sprememb.

2. Področje uporabe

2.1 Ta politika velja za:

2.1.1 zaposlene in vodje oddelkov, ki predlagajo ali izvajajo spremembe,

2.1.2 zunanje ponudnike IT-storitev, ki upravljajo sisteme ali programsko opremo,

2.1.3 generalnega direktorja, ki nosi splošno odgovornost za odobravanje sprememb.

2.2 Ta politika zajema spremembe:

2.2.1 programske opreme (posodobitve, popravki, nove aplikacije),

2.2.2 strojne opreme (zamenjave, nadgradnje),

2.2.3 omrežnih konfiguracij in konfiguracij požarnih zidov,

2.2.4 storitev v oblaku, pravic dostopa uporabnikov ali integracij z dobavitelji,

2.2.5 kritičnih sprememb poslovnih procesov, ki vključujejo informacijske sisteme.

2.3 V področje uporabe te politike sodijo tako načrtovane kot nujne spremembe.

3. Cilji

3.1 Zagotoviti, da so vse spremembe IT- in poslovnih sistemov odobrene, dokumentirane ter povrnjive, če pride do težav.

3.2 Preprečiti nenačrtovane izpade, izgubo podatkov ali varnostne incidente, ki jih povzročijo nenadzorovane spremembe.

3.3 Določiti enostavne in ponovljive postopke za oddajo zahtevka za spremembo, odobritev, testiranje in povrnitev.

3.4 Vzdrževati preverljiv dnevnik sprememb, ki podpira operativno odgovornost in regulativno skladnost.

3.5 Omogočiti odločanje na podlagi tveganj za pomembne ali občutljive spremembe.

4. Vloge in odgovornosti

4.1 Generalni direktor

4.1.1 Nosi končno odgovornost za vse večje spremembe.

4.1.2 Pregleduje in odobrava nerutinske, kritične ali visoko tvegane spremembe.

4.1.3 Četrtletno ali po večjih incidentih pregleda dnevnik sprememb.

4.2 IT-podpora ali zunanji ponudnik IT-storitev

4.2.1 Izvaja spremembe, vključno s posodobitvami konfiguracij, nameščanjem popravkov in migracijami sistemov.

4.2.2 Vzdržuje osnovni dnevnik sprememb, ki vsebuje datume, vrste sprememb, rezultate in odobritelje.

4.2.3 Pred izvedbo testira spremembe in po potrebi izvede postopke povrnitve.

4.2.4 Obvesti prizadete uporabnike pred večjimi spremembami in po njih.

[... 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 Letni pregled

9.1.1 To politiko mora generalni direktor ali določena kontaktna oseba za IT pregledati najmanj enkrat letno, da se zagotovi usklajenost z aktualnimi sistemi, delovnimi poteki in regulativnimi zahtevami.

9.2 Vmesni pregledi

9.2.1 Pregledi se morajo izvesti tudi zaradi:

9.2.1.1 varnostnih incidentov, povzročenih zaradi neustreznega upravljanja sprememb,

9.2.1.2 uvedbe novih IT-sistemov,

9.2.1.3 sprememb ustreznih standardov, kot so ISO, NIS2 ali DORA.

9.3 Dokumentiranje posodobitev

9.3.1 Spremembe te politike morajo biti različicno vodene in odobrene s strani generalnega direktorja. Vsaka različica mora vsebovati datum, povzetek sprememb in odobritelja.

9.4 Sporočanje politike

9.4.1 Vse posodobitve morajo biti sporočene vsem prizadetim zaposlenim in zunanjim ponudnikom. Dokumentacija mora biti posodobljena na vseh referenčnih lokacijah (npr. kadrovski portal, deljeni diski).

10. Povezane politike in povezave

10.1 Ta politika je tesno povezana z naslednjimi politikami za SME:

10.1.1 P2S – Politika vlog in odgovornosti upravljanja: določa pooblastila za odobravanje sprememb.

10.1.2 P4S – Politika nadzora dostopa: zagotavlja, da so spremembe dostopa, ki izhajajo iz sprememb, pravilno dokumentirane in izvedene.

10.1.3 P7S – Politika uvajanja in prenehanja sodelovanja: usklajuje spremembe, povezane s prehodi med vlogami in dodeljevanjem dostopa.

10.1.4 P15S – Politika varnostnega kopiranja in obnovitve: zagotavlja, da je mogoče v primeru neuspešne spremembe izvesti povrnitev in obnovitev.

10.1.5 P30S – Politika odzivanja na incidente: določa, kako se neuspešne ali nepooblaščene spremembe obravnavajo kot varnostni incidenti.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 6.1 – načrtovanje na podlagi tveganj mora vključevati dejavnosti, povezane s spremembami.

11.1.2 Klavzula 8.1 – operativne kontrole se morajo dosledno uporabljati pri dejavnostih, povezanih s spremembami, da se zagotovi celovitost storitev.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.32 – podaja smernice za varne procese upravljanja sprememb, vključno z dokumentiranjem, testiranjem in odobravanjem.

11.3 NIST SP 800-53 Rev. 5

11.3.1 CM-2 – izhodiščna konfiguracija sistemov pred spremembo.

11.3.2 CM-3 – nadzor sprememb konfiguracije.

11.3.3 CM-4 – analiza varnostnega vpliva.

11.3.4 CM-5 – odobravanje in dokumentiranje sprememb.

11.3.5 CM-11 – revizija in spremljanje sprememb.

11.4 Direktiva EU NIS2

11.4.1 Člen 21(2)(b) – zahteva formalne postopke za tehnične in organizacijske varnostne ukrepe, vključno z upravljanjem sprememb.

11.5 Uredba EU DORA

11.5.1 Člena 6(9) in 8(4)(b) – od finančnih subjektov zahtevata vzdrževanje upravljanja sprememb in upravljanja konfiguracij za sisteme IKT.

11.6 COBIT 2019

11.6.1 BAI06 – Upravljanje sprememb: poudarja načrtovanje, oceno tveganj in zmožnost povrnitve.

11.6.2 DSS01 – Upravljanje operacij: zagotavlja operativno celovitost med tehničnimi prehodi in spremembami.