					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P05					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	Klavzuli 6.1, 5.15	Obravnava ukrepe za obvladovanje tveganj, nadzor dostopa in upravljanje sprememb
ISO/IEC 27002:2022	Kontrola 8	Uvaja strukturiran proces upravljanja sprememb
NIST SP 800-53 Rev.5	CM-2 do CM-14	Kontrole upravljanja konfiguracije
EU GDPR	Členi 32(1)(b–d), 25; uvodna izjava 78	Tehnični in organizacijski ukrepi za varnost sistemov in podatkov med spremembami
EU NIS2	Člen 21(2)(a, b, d, e)	Zahteva obvladovanje tveganj sprememb IKT
EU DORA	Členi 5, 8, 12	Ureja operativna tveganja in tveganja IKT ter poročanje o incidentih
COBIT 2019	BAI06, BAI02, BAI03, DSS01, MEA01, MEA03	Strukturirano upravljanje sprememb IT, spremljanje uspešnosti, skladnost in zahteve

1. Namen

1.1. Ta politika določa formalni okvir za začetek, presojo, odobritev, izvedbo in pregled sprememb informacijskih sistemov, infrastrukture, aplikacij in povezanih procesov organizacije.

1.2. Zagotavlja, da se vse spremembe izvajajo nadzorovano in na revizijsko ustrezen način, pri čemer se zmanjšuje tveganje motenj, ogrožanja varnosti ali regulatorne neskladnosti.

1.3. Podpira kontrolo 8.32 iz Priloge A standarda ISO/IEC 27001:2022 z uveljavitvijo varnih, dokumentiranih praks upravljanja sprememb, usklajenih s tveganji.

1.4. Politika zagotavlja tudi sledljivost odločitev o spremembah in krepi operativno odpornost med načrtovanimi ali nujnimi spremembami.

2. Področje uporabe

2.1. Ta politika se uporablja za vse spremembe, ki vplivajo na sisteme, podatke in okolja znotraj obsega ISMS, vključno z:

2.1.1. IT infrastrukturo (v lastnih okoljih, v oblaku, hibridno)

2.1.2. produkcijskimi, predprodukcijskimi in okolji za obnovitev po nesreči

2.1.3. poslovnimi aplikacijami, storitvami, programskimi vmesniki API in integracijami

2.1.4. nastavitvami konfiguracije, nameščanjem popravkov, izdajami programske opreme in migracijami sistemov

2.1.5. nujnimi popravki ter projektnimi ali načrtovanimi spremembami

2.2. Ureja spremembe, ki jih sprožijo:

2.2.1. interno osebje (IT operacije, razvijalci, lastniki sistemov)

2.2.2. zunanji dobavitelji, ponudniki upravljanih storitev (MSP) in pogodbeni izvajalci

2.2.3. projektne ekipe med uvajanjem sistemov, nadgradnjami ali prehodi storitev

2.3. Ta politika se ne uporablja za:

2.3.1. začasna testna ali razvojna okolja brez dostopa do produkcijskih podatkov

2.3.2. osebne uporabniške konfiguracije (urejene v okviru Politike sprejemljive uporabe (AUP))

2.3.3. spremembe sistemov zunaj meje nadzora organizacije, razen če vplivajo na integrirana sredstva ali obveznosti skladnosti

3. Cilji

3.1. Zagotoviti, da so vse spremembe pred izvedbo pregledane, odobrene, testirane in dokumentirane.

3.2. Ohranjati razpoložljivost sistemov, celovitost podatkov in neprekinjenost storitev med dejavnostmi sprememb in po njih.

3.3. Zahtevati opredeljene klasifikacije sprememb, načrte povrnitve in ocene tveganja za vse vrste sprememb.

3.4. Omogočiti pregledno odločanje in eskalacijo s strukturiranim upravljanjem.

3.5. Podpirati pripravljenost na revizijo s sledljivimi zapisi o spremembah in pregledi po izvedbi.

3.6. Uveljaviti ločevanje dolžnosti (SoD) ter zmanjšati tveganje nepooblaščenih ali nasprotujočih si sprememb v kritičnih sistemih.

4. Vloge in odgovornosti

4.1. Najvišje vodstvo

4.1.1. Potrjuje P05 Politiko upravljanja sprememb in zagotavlja usklajenost s strateškimi cilji ter regulatornimi obveznostmi.

4.1.2. V okviru upravljavskega nadzora odobrava programe sprememb z velikim vplivom ali medfunkcijskim učinkom.

4.1.3. Dodeljuje potrebne vire in proračun za orodja za nadzor sprememb ter usposabljanje osebja.

4.2. Odbor za odobritev sprememb (CAB)

4.2.1. Pregleduje in odobrava standardne ter večje spremembe ter zagotavlja ustrezno presojo tveganj, vplivov in odvisnosti.

4.2.2. Potrjuje načrte povrnitve, rezultate testiranja, komunikacijo z deležniki in razporejanje.

4.2.3. Sestavljajo ga lastniki sistemov, predstavniki informacijske varnosti, IT operacij, poslovni vodje in predstavniki za skladnost.

4.2.4. Pod dokumentiranimi pogoji lahko delegira odločitve za nizkotvegane ali nujne spremembe.

[... 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. Sprožilci pregleda in pogostost

9.1.1. Ta politika mora biti pregledana letno ali ob:

9.1.1.1. večjih spremembah IT ali infrastrukture

9.1.1.2. pomembnih incidentih, povezanih z neuspešnimi ali nepooblaščenimi spremembami

9.1.1.3. regulatornih posodobitvah ali novih pravnih obveznostih, povezanih s spremembami

9.1.1.4. uvedbi novih orodij ali platform sistema za upravljanje sprememb

9.2. Postopek pregleda Politike upravljanja sprememb

9.2.1. Vodja sprememb vodi postopek pregleda v sodelovanju z:

9.2.1.1. IT, informacijsko varnostjo in operacijami

9.2.1.2. notranjo revizijo in upravljanjem tveganj

9.2.1.3. predstavniki CAB

9.2.2. Posodobitve morata pregledati in odobriti najvišje vodstvo ter usmerjevalni odbor ISMS.

9.2.3. Ponovno izdane različice morajo biti evidentirane v registru dokumentov in posredovane prizadetim stranem, pri čemer se po potrebi zahteva ponovno potrjevanje seznanitve.

9.3. Nadzor dokumentov in upravljanje različic

9.3.1. Vse različice morajo vključevati:

9.3.1.1. ID politike, naslov in raven razvrstitve

9.3.1.2. lastnika in evidenco različic

9.3.1.3. dnevnik sprememb in datum začetka veljavnosti

9.3.1.4. organ odobritve

9.3.2. Arhivirane različice se morajo hraniti v skladu s Politiko hrambe dokumentov (najmanj 3 leta).

10. Povezane politike in povezave

10.1. Ta politika je neposredno povezana z izvajanjem naslednjih politik in ga podpira:

10.1.1. P1 – Politika informacijske varnosti: Določa zahtevo po formalnih varnostnih kontrolah in odgovornostih na ravni procesov, vključno z upravljanjem sprememb.

10.1.2. P2 – Politika vlog in odgovornosti upravljanja: Opredeljuje pristojnosti za odobritev in ločevanje dolžnosti (SoD), pomembne za odobritev sprememb in nadzor.

10.1.3. P4 – Politika nadzora dostopa: Zagotavlja, da dovoljenja dostopa za izvajalce sprememb in pregledovalce sledijo načelu najmanjših privilegijev.

10.1.4. P6 – Politika upravljanja tveganj: Zagotavlja, da so vse spremembe predmet ustrezne ocene tveganja in strategij za ublažitev.

10.1.5. P33 – Politika spremljanja revizije in skladnosti: Ureja validacijo in revizijski pregled zapisov upravljanja sprememb ter kršitev.

10.2. Te politike skupaj omogočajo utemeljen, sledljiv in varen življenjski cikel upravljanja sprememb v okviru ISMS.

11. Referenčni standardi in okviri

11.1. ISO/IEC 27001:2022

11.1.1. Klavzula 6.1 – Ukrepi za obravnavo tveganj in priložnosti: Ta politika podpira identifikacijo, oceno in obvladovanje tveganj, povezanih s spremembami.

11.1.2. Klavzula 5.15 – Nadzor dostopa: Zagotavlja, da je dostop med spremembami nadzorovan in sledljiv.

11.1.3. Priloga A, kontrola 8.32 – Upravljanje sprememb: Ta politika v celoti izvaja zahtevo po upravljanju sprememb naprav za obdelavo informacij in sistemov na načrtovan in nadzorovan način.

11.2. ISO/IEC 27002:2022 – Kontrola 8

11.2.1. Krepi izvajanje strukturiranega procesa upravljanja sprememb, vključno s klasifikacijo sprememb, odobritvijo, testiranjem, povrnitvijo in dokumentiranjem.

11.3. NIST SP 800-53 Rev.5

11.3.1. Družina CM (CM-1 do CM-14): Ta politika je tesno usklajena s kontrolami upravljanja konfiguracije, vključno z izhodiščnimi konfiguracijami (CM-2), nadzorom sprememb konfiguracije (CM-3), analizo varnostnega vpliva (CM-4) in omejitvami dostopa (CM-5).

11.3.2. Družina AU (AU-2, AU-6, AU-12): Mehanizmi beleženja in revizije, navedeni v tej politiki, podpirajo sledljivost dogodkov in pregled skladnosti za dejavnosti, povezane s spremembami.

11.3.3. RA-3, RA-5: Ocene tveganja, ki jih sprožijo spremembe, in skeniranje ranljivosti so vključeni v proces vrednotenja sprememb.

11.3.4. PM-11 (Opredelitev poslanstva/poslovnega procesa): Zagotavlja, da se med spremembami ohranjata neprekinjeno poslovanje in operativni cilji.

11.4. EU GDPR (2016/679)

11.4.1. Člen 32(1)(b–d): Ta politika podpira zahtevo po ustreznih tehničnih in organizacijskih ukrepih za zagotavljanje varnosti podatkov, zlasti med spremembami sistemov.

11.4.2. Člen 25 – Vgrajeno in privzeto varstvo podatkov: Zagotavlja, da spremembe, ki vplivajo na osebne podatke, vključujejo zasebnost in varnost v zasnovo ter uvedbo.

11.4.3. Uvodna izjava 78: Zahteva, da upravljavci podatkov uvedejo mehanizme, kot so politike nadzora sprememb, za zagotavljanje stalne zaupnosti, celovitosti in odpornosti sistemov obdelave.

11.5. Direktiva EU NIS2 (2022/2555)

11.5.1. Člen 21(2)(a, b, d, e): Zahteva tehnične in organizacijske ukrepe za obvladovanje tveganj IKT, vključno s tveganji, ki izhajajo iz sprememb sistemov, posodobitev programske opreme in sprememb infrastrukture.

11.6. Uredba EU DORA (2022/2554)

11.6.1. Člen 5 – Okvir upravljanja in notranjih kontrol: Ta politika uveljavlja načela upravljanja operativnih tveganj, povezana s spremembami in posodobitvami IKT.

11.6.2. Člen 8 – Okvir za obvladovanje tveganj IKT: Zahteva, da finančni subjekti vse spremembe, ki vplivajo na sisteme IKT, upravljajo v okviru strukturiranih procesov upravljanja sprememb, kar se v tej politiki odraža v zahtevah glede klasifikacije, testiranja, povrnitve in dokumentiranja.

11.6.3. Člen 12 – Poročanje o incidentih: Zagotavlja, da so neuspele spremembe, ki povzročijo motnje IKT, sledljive, dokumentirane in po potrebi prijavljene.

11.7. COBIT 2019

11.7.1. BAI06 – Upravljane spremembe IT: Ta politika neposredno izpolnjuje cilje BAI06 z določitvijo strukturiranih delovnih tokov za odobritev sprememb, presojo vpliva, komunikacijo in testiranje.

11.7.2. BAI02 – Upravljano opredeljevanje zahtev in BAI03 – Upravljana identifikacija in razvoj rešitev: Zagotavljata, da se poslovno vodene spremembe varno pregledajo in uvedejo.

11.7.3. DSS01 – Upravljane operacije: Podpira stalno celovitost sistemov med izvajanjem sprememb.

11.7.4. MEA01 in MEA03 – Spremljanje, vrednotenje in ocenjevanje uspešnosti ter skladnosti: Omogoča stalni nadzor nad učinkovitostjo in upoštevanjem politike upravljanja sprememb.