					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P37S					Naslov dokumenta: **Politika pravne in regulativne skladnosti**							
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**

Pravno obvestilo (avtorske pravice in omejitve uporabe)

(C) 2025 Clarysec LLC. All rights reserved.

Ta dokument je intelektualna lastnina družbe Clarysec LLC. Noben del tega dokumenta se ne sme kopirati, ponovno uporabiti, distribuirati ali spreminjati za komercialne ali implementacijske namene brez predhodnega izrecnega pisnega dovoljenja.

Nepooblaščena uporaba je strogo prepovedana in lahko povzroči pravne ukrepe.

Za licenciranje se obrnite na: info@clarysec.com

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
ISO/IEC 27001:2022	Klavzule 5.1, 6.1, 6.2, 8	
ISO/IEC 27002:2022	Kontrola 5	
NIST SP 800-53 Rev. 5	PL-1, PL-2, PM-1, CA-1, AU-1	
Uredba (EU) GDPR	Členi 5, 6, 32, 33	
Direktiva (EU) NIS2	Členi 21(2)(a), 21(2)(f), 23	
Uredba (EU) DORA	Členi 5(2), 9(1), 17	
COBIT 2019	APO12, APO13, DSS01	

1. Namen

1.1 Ta politika določa pristop organizacije k prepoznavanju, izpolnjevanju in izkazovanju skladnosti s pravnimi, regulativnimi in pogodbenimi obveznostmi.

1.2 Določa jasne odgovornosti in praktične korake za podporo poslovanju pri izpolnjevanju obveznosti skladnosti, vključno z zakonodajo o varstvu podatkov, okviri kibernetske varnosti, pogodbami s strankami in certifikacijskimi standardi.

1.3 Zagotavlja, da lahko organizacija tudi brez namenske funkcije skladnosti vzdržuje pravno skladno poslovanje, se ustrezno odziva na incidente in ohranja pripravljenost na presoje.

1.4 Ta politika je bistvena za podporo certificiranju po standardu ISO/IEC 27001:2022 in za izpolnjevanje zunanjih pričakovanj strank, regulatorjev in partnerjev.

2. Področje uporabe

2.1 Ta politika se uporablja za:

2.1.1 vse zaposlene, pogodbene izvajalce, samostojne podjetnike in dobavitelje tretjih oseb;

2.1.2 vse storitve, procese, sisteme in dejavnosti obdelave podatkov, pri katerih mora organizacija izpolnjevati pravne ali pogodbene zahteve;

2.1.3 vse lokacije in naprave, ki se uporabljajo za obdelavo poslovnih informacij, ne glede na to, ali gre za pisarniško okolje, delo na daljavo ali sisteme v oblaku.

2.2 Politika zajema:

2.2.1 zakonodajo o varstvu podatkov, kot je Uredba (EU) GDPR;

2.2.2 predpise s področja kibernetske varnosti, kot je Direktiva (EU) NIS2;

2.2.3 obveznosti, specifične za posamezni sektor, kadar je to relevantno;

2.2.4 pogodbe s strankami, sporazume o nerazkrivanju informacij in revizijske klavzule;

2.2.5 prostovoljne certifikacije (npr. ISO/IEC 27001) in interne politike, ki jih je treba izvajati zaradi zagotavljanja skladnosti.

3. Cilji

3.1 Vzpostavitev odgovornosti: dodeliti jasno odgovornost za spremljanje, posodabljanje in uveljavljanje pravnih, regulativnih in pogodbenih obveznosti.

3.2 Zaščita poslovanja: zmanjšati tveganje pravnih kršitev, glob, kršitev varstva osebnih podatkov in škode za ugled.

3.3 Zagotavljanje pripravljenosti na presoje: vzdrževati preverljive evidence, ki izkazujejo, kako organizacija izpolnjuje svoje obveznosti glede skladnosti.

3.4 Podpora integraciji politik: zagotoviti, da se pravne in regulativne obveznosti dosledno odražajo v vseh politikah in procesih.

3.5 Pregledno upravljanje izjem: zagotoviti, da so vse izjeme glede skladnosti dokumentirane, utemeljene in odobrene, da se prepreči nastanek odgovornosti.

4. Vloge in odgovornosti

4.1 Generalni direktor

4.1.1 Nosi celotno odgovornost za pravno in regulativno skladnost organizacije.

4.1.2 Vodi evidenco skladnosti in zagotavlja njeno ažurnost.

4.1.3 Pregleduje pogodbe s strankami ter zagotavlja, da so posebne obveznosti evidentirane in uveljavljene.

4.1.4 Odobri izjeme od obveznosti skladnosti le, kadar so pravno utemeljene in kadar so uvedene nadomestne kontrole.

4.2 Zunanji svetovalci (npr. pravni, IT ali svetovalci za skladnost)

4.2.1 Generalnemu direktorju nudijo podporo pri prepoznavanju veljavne zakonodaje, certifikacij in obveznosti (npr. GDPR, NIS2, ISO/IEC 27001).

4.2.2 Podajajo usmeritve za razlago novih predpisov ali sprememb obstoječe zakonodaje.

4.2.3 Po potrebi lahko pomagajo pri posodobitvah politik, presojah ali odzivu na kršitve, kadar obstaja pravna izpostavljenost.

[... 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 Načrtovani letni pregled

9.1.1 To politiko mora generalni direktor pregledati vsakih 12 mesecev.

9.1.2 Pregled mora potrditi:

9.1.2.1 ustreznost glede na veljavni pravni in pogodbeni okvir;

9.1.2.2 pravilno upoštevanje dogovorov s strankami in obveznosti izvajanja storitev;

9.1.2.3 usklajenost z evidenco skladnosti in drugimi politikami.

9.2 Posodobitve na podlagi dogodkov

9.2.1 Takojšnji pregled je potreben, če:

9.2.1.1 začne veljati nov zakon ali predpis (npr. novo pravilo s področja varstva podatkov);

9.2.1.2 stranka v pogodbo doda strožja določila glede skladnosti;

9.2.1.3 pride do kršitve ali incidenta neskladnosti;

9.2.1.4 podjetje razširi poslovanje na reguliran trg ali v reguliran sektor.

9.3 Odobritev posodobitev in nadzor različic

9.3.1 Vse posodobitve morajo biti dokumentirane, označene s številko različice in odobrene s strani generalnega direktorja.

9.3.2 Zgodovinske različice morajo biti hranjene za revizijske in pravne namene.

9.4 Obveščanje o spremembah

9.4.1 Zaposleni in pogodbeni izvajalci morajo biti o spremembah politike obveščeni v 5 delovnih dneh po odobritvi.

9.4.2 Vsi zadevni dobavitelji morajo pred nadaljnjim izvajanjem storitev potrditi tudi posodobljene pogoje.

10. Povezane politike in povezave

10.1 To politiko podpirajo in uveljavljajo naslednje politike SME:

10.1.1 P3S – Politika dopustne uporabe (AUP): preprečuje ravnanja, ki bi lahko kršila pravne ali pogodbene določbe (npr. nepooblaščeno deljenje datotek).

10.1.2 P8S – Politika ozaveščanja in usposabljanja za informacijsko varnost: seznanja osebje z obveznostmi skladnosti in načini preprečevanja kršitev.

10.1.3 P14S – Politika hrambe podatkov in odstranjevanja: zagotavlja zakonite prakse ravnanja s podatki skozi celoten življenjski cikel podatkov.

10.1.4 P17S – Politika varstva podatkov in zasebnosti: izpolnjuje zahteve GDPR in zahteve strank glede ravnanja s podatki.

10.1.5 P30S – Politika odzivanja na incidente: določa način odzivanja na kršitve varnosti osebnih podatkov ali primere neskladnosti, vključno z roki za obveščanje.

10.1.6 P36S – Politika družbenih medijev in zunanjega komuniciranja: zagotavlja, da javno komuniciranje ne krši pravnih ali regulativnih obveznosti.

10.2 Vsaka povezana politika uveljavlja del okvira pravne skladnosti in se mora uporabljati usklajeno z drugimi.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 6.1 – ukrepi za obravnavo tveganj in priložnosti: vključuje tveganja skladnosti.

11.1.2 Klavzula 8.1 – operativno načrtovanje in nadzor: zahteva izvajanje procesov, ki izpolnjujejo pravne in pogodbene zahteve.

11.2 ISO/IEC 27002

11.2.1 Kontrola 5.36 – usmerja organizacijo pri vodenju evidenc obveznosti in zagotavljanju ustreznega odzivanja na pravne in regulativne zahteve.

11.3 NIST SP 800-53 Rev. 5

11.3.1 PL-1 – politika in postopki: zahteva formalne politike skladnosti.

11.3.2 PM-1 – načrt programa informacijske varnosti: zahteva vključitev pravne skladnosti v načrtovanje informacijske varnosti.

11.3.3 CA-1 – presoja, odobritev in spremljanje.

11.3.4 AU-1 – revizijska politika: zahteva vzdrževanje dokazil o skladnosti.

11.4 Uredba (EU) GDPR

11.4.1 Člen 5 – načela obdelave osebnih podatkov, vključno z odgovornostjo.

11.4.2 Člen 6 – pravna podlaga za obdelavo.

11.4.3 Člen 32 – varnost obdelave.

11.4.4 Člen 33 – prijava kršitve v 72 urah.

11.5 Direktiva (EU) NIS2

11.5.1 Člen 21(2)(a) in (f) – interne politike za obvladovanje tveganj in regulativni nadzor.

11.5.2 Člen 23 – uveljavljanje in sankcije za neskladnost.

11.6 Uredba (EU) DORA

11.6.1 Člen 5(2) – nadzor nad upravljanjem tveganj IKT.

11.6.2 Člen 9(1) – interno upravljanje skladnosti.

11.6.3 Člen 17 – pogodbene ureditve s ponudniki storitev IKT.

11.7 COBIT 2019

11.7.1 APO12 – upravljano tveganje: zagotavlja, da se tveganja skladnosti spremljajo in obravnavajo.

11.7.2 APO13 – upravljana varnost: zajema uveljavljanje regulativne in pogodbene skladnosti na podlagi tveganj.

11.7.3 DSS01 – upravljane operacije: zahteva operativno pripravljenost za izpolnjevanje pravnih obveznosti.