					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P33					Naslov dokumenta: **Politika spremljanja presoj in 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**

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
ISO/IEC 27001:2022	Klavzule 9.2, 9.3, 10	
ISO/IEC 27002:2022	Kontrole 5.35–5.37	
NIST SP 800-53 Rev.5	CA-2, CA-5, CA-7	
Uredba EU GDPR	Členi 24, 32, 33	
Direktiva EU NIS2	Člena 21(2)(g), 27	
Uredba EU DORA	Člena 10(2)(e), 25	
COBIT 2019	MEA01, MEA03	

1. Namen

1.1 Namen te politike je vzpostaviti in urediti program spremljanja presoj in skladnosti organizacije, da se:

1.1.1 preveri učinkovitost varnostnih kontrol in kontrol zasebnosti

1.1.2 zagotovi skladnost z veljavnimi standardi, pravnimi okviri in pogodbenimi obveznostmi

1.1.3 pravočasno zaznajo neskladnosti, neučinkovitosti in tveganja neskladnosti

1.1.4 podpre nenehno izboljševanje ter pripravljenost na certifikacije, presoje in regulativne preglede

1.2 Ta politika podpira celovitost in zaupnost ter zrelost sistema upravljanja informacijske varnosti (ISMS), tako da vzpostavlja strukturirane, na tveganjih temelječe in z dokazi podprte prakse presoje in spremljanja.

2. Področje uporabe

2.1 Ta politika se uporablja za vse:

2.1.1 notranje poslovne enote, funkcije in oddelke

2.1.2 fizične lokacije, okolja v oblaku, platforme SaaS in zunanje izvajane storitve

2.1.3 informacijske sisteme, aplikacije, infrastrukturo in podatkovna sredstva, ki jih ureja ISMS

2.1.4 zaposlene, pogodbene izvajalce in tretje ponudnike storitev z obveznostmi v zvezi s presojo ali skladnostjo

2.2 Politika zajema:

2.2.1 notranje presoje

2.2.2 zunanje/certifikacijske presoje

2.2.3 tehnično spremljanje skladnosti

2.2.4 presoje dobaviteljev in tretjih oseb

2.2.5 korektivne in preventivne ukrepe (CAPA)

2.2.6 kazalnike, nadzorne plošče in procese poročanja

2.3 Uporablja se za vse ustrezne okvire, ki zavezujejo organizacijo, med drugim ISO/IEC 27001, GDPR, NIS2, DORA in SOC 2.

3. Cilji

3.1 Preveriti ustreznost in učinkovitost uvedenih kontrol, politik in postopkov v celotnem ISMS in povezanih okoljih.

3.2 Prepoznati in odpraviti vse pomanjkljivosti, neskladnosti ali vrzeli v skladnosti, preden prerastejo v incidente ali kršitve.

3.3 Zagotoviti trajno pripravljenost na notranje vodstvene preglede, zunanje presoje in neodvisne certifikacije.

3.4 Ustvarjati preverljiva dokazila in revizijsko sled za podporo pri poizvedbah regulatorjev, pravnih postopkih ali zahtevah strank glede zagotavljanja skladnosti.

3.5 Vključevati rezultate presoj v širše dejavnosti organizacije na področju obvladovanja tveganj, varnostnih kazalnikov in nenehnega izboljševanja.

4. Vloge in odgovornosti

4.1 Vodja notranje revizije / vodja skladnosti

4.1.1 Na podlagi prioritet tveganj načrtuje, razporeja in izvaja notranje presoje.

4.1.2 Vodi evidenco presoj, usklajuje dejavnosti presoje in spremlja korektivne ukrepe.

4.2 Vodja informacijske varnosti (CISO)

4.2.1 Zagotavlja, da obseg presoje zajema vse ustrezne elemente ISMS in kontrole iz Priloge A.

4.2.2 Nadzira preverjanje CAPA in vključuje rezultate presoj v varnostni program.

[... 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 To politiko morata najmanj enkrat letno pregledati vodja skladnosti in vodja informacijske varnosti (CISO), ali prej kot odziv na:

9.1.1 spremembe v regulativnih, pogodbenih ali certifikacijskih okvirih

9.1.2 pomembne ugotovitve presoj ali ponavljajoče se odpovedi kontrol

9.1.3 organizacijsko prestrukturiranje ali spremembe sistema GRC

9.1.4 priporočila zunanjih presojevalcev ali povratne informacije regulatorjev

9.2 Postopek pregleda mora presoditi:

9.2.1 metodologijo in pogostost načrtovanja presoj

9.2.2 spremembe obsega ISMS ali infrastrukture

9.2.3 posodobitve kataloga kontrol ali pravnega registra

9.2.4 doslednost in kakovost revizijskih dokazil ter procesov CAPA

9.3 Vse spremembe politike morajo biti:

9.3.1 dokumentirane v repozitoriju, upravljanem z različicami

9.3.2 odobrene s strani najvišjega vodstva

9.3.3 sporočene vsem prizadetim zaposlenim in vključene v posodobljene postopke ter programe ozaveščanja

9.4 Potrditev po pregledu mora zagotoviti, da se posodobljene zahteve odražajo v evidenci presoj, orodjih za skladnost in notranjih nadzornih ploščah za spremljanje.

10. Povezane politike in povezave

10.1 Ta politika je usklajena z naslednjimi povezanimi organizacijskimi politikami:

10.1.1 P1 – Politika informacijske varnosti: opredeljuje ISMS in določa odgovornost za skladnost ter nenehno izboljševanje

10.1.2 P5 – Politika upravljanja sprememb: zagotavlja preglednost sprememb infrastrukture in konfiguracij, ki vplivajo na kontrolna okolja v okviru presoj

10.1.3 P6 – Politika upravljanja tveganj: vključuje rezultate presoj v korporativno ocenjevanje tveganj in dejavnosti obravnave tveganj

10.1.4 P14 – Politika hrambe podatkov in odstranjevanja: ureja hrambo revizijskih dokazil, dnevnikov in evidenc skladnosti

10.1.5 P18 – Politika kriptografskih kontrol: podpira varno shranjevanje in prenos občutljivih revizijskih podatkov

10.1.6 P26 – Politika varnosti dobaviteljev: zajema pravice do revizije, dokumentacijo o zagotovilih in nadzor skladnosti dobaviteljev

10.1.7 P30 – Politika odzivanja na incidente: usklajuje presoje postopkov obravnave incidentov s cilji zagotavljanja ISMS

10.1.8 P32 – Politika neprekinjenega poslovanja in obnove po nesrečah: zahteva preverjanje testiranja neprekinjenega poslovanja in skladnosti DRP v ciklih presoj

11. Referenčni standardi in okviri

11.1 Ta politika je usklajena z globalnimi standardi in pravnimi zahtevami za presoje in stalno preverjanje skladnosti.

11.2 ISO/IEC 27001:

11.2.1 Klavzula 9.2 – Notranja presoja: zahteva redne presoje ISMS na podlagi tveganj za ocenjevanje učinkovitosti in skladnosti.

11.2.2 Klavzula 9.3 – Vodstveni pregled: rezultati presoje morajo prispevati k strateškemu pregledu in izboljševanju.

11.2.3 Klavzula 10.1 – Neskladnost in korektivni ukrep: ugotovitve presoje morajo biti obravnavane z dokumentiranimi postopki CAPA.

11.3 ISO/IEC 27002:2022 – Kontrole 5.35–5.37:

11.3.1 Kontrole iz Priloge A 5.35–5.37: zajemajo neodvisni pregled, skladnost s pravnimi in pogodbenimi zahtevami ter revizijsko beleženje.

11.3.2 Določajo smernice za načrtovanje, izvedbo in izboljševanje programov presoje in skladnosti.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CA-2 – Presoje kontrol: zahteva rutinski pregled uvedenih varnostnih kontrol.

11.4.2 CA-5 – Plan of Action and Milestones (POA&M): usklajen je s spremljanjem in odpravo ugotovitev presoje.

11.4.3 CA-7 – Stalno spremljanje: podpira proaktivne, avtomatizirane presoje skladnosti.

11.5 Uredba EU GDPR (2016/679):

11.5.1 Člena 24 in 32: zahtevata dokazila o uvedbi in učinkovitosti varnostnih kontrol prek ustreznih struktur upravljanja.

11.5.2 Člen 33: podpira potrebo po preverljivi revizijski sledi pri odzivu na kršitve in obveščanju.

11.6 Direktiva EU NIS2 (2022/2555):

11.6.1 Člen 21(2)(g): zahteva presojo politik in postopkov kot del minimalnih ukrepov za obvladovanje tveganj kibernetske varnosti.

11.6.2 Člen 27: nacionalni organi lahko izvajajo presoje ali jih zahtevajo za bistvene in pomembne subjekte.

11.7 Uredba EU DORA (2022/2554):

11.7.1 Člen 10(2)(e): subjekti morajo izvajati notranje in zunanje presoje praks upravljanja tveganj IKT.

11.7.2 Člen 25 – Zahteve glede presoj: zahteva periodične presoje, ki jih izvajajo notranji ali neodvisni zunanji presojevalci ob regulatorni vidljivosti.

11.8 COBIT 2019:

11.8.1 MEA01 – Nadzor, vrednotenje in ocenjevanje uspešnosti ter skladnosti: zagotavlja, da se učinkovitost kontrol preverja in o njej poroča organom upravljanja.

11.8.2 MEA03 – Nadzor, vrednotenje in ocenjevanje skladnosti: zahteva uskladitev organizacijskih praks s pravnimi, pogodbenimi in standardnimi zahtevami.