					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P33S					Naslov dokumenta: **Politika revizij in spremljanja skladnosti P33S**							
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 9.2, 10	Notranje revizije, nenehno izboljševanje in odprava neskladnosti
ISO/IEC 27002:2022	Kontroli 5.35, 5.37	Načrtovani notranji pregledi, neodvisni pregledi zunanje izvajanih procesov
NIST SP 800-53 Rev.5	CA-2, CA-7, AU-6	Varnostne presoje, neprekinjeno spremljanje ter pregled, analiza in poročanje o revizijskih zapisih
Uredba EU GDPR	Člena 24 in 32	Revidiranje tehničnih in organizacijskih ukrepov ter dokazila o učinkovitosti kontrol
Direktiva EU NIS2	Člen 21(2)(f)	Proaktivni pregled in dokazljivo izkazana skladnost
Uredba EU DORA	Člen 10	Upravljanje tveganj IKT, spremljanje in poročanje
COBIT 2019	MEA01, MEA03	Spremljanje in presoja skladnosti ter pripravljenost na preglede tretjih oseb

1. Namen

1.1 Ta politika določa pristop organizacije k izvajanju notranjih revizij, preverjanju varnostnih kontrol in spremljanju regulativne skladnosti. Zagotavlja, da so vse kontrole, politike, sistemi in zunanji izvajalci storitev redno in strukturirano pregledovani.

1.2 Namen politike je odkriti odpovedi kontrol, preprečiti neskladnost in izkazati dolžno skrbnost v skladu z ISO/IEC 27001, GDPR in povezanimi okviri.

1.3 Ta politika MSP omogoča ohranjanje operativnega nadzora in pripravljenosti na certifikacijo tudi brez namenskega oddelka za skladnost, z uporabo preprostih, ponovljivih kontrolnih seznamov in ugotovitev, prednostno obravnavanih glede na tveganje.

2. Področje uporabe

2.1 Ta politika velja za:

2.1.1 vse notranje oddelke in zunanje izvajalce storitev, ki imajo odgovornosti v zvezi s sistemi IT, osebnimi podatki in poslovno kritičnimi storitvami,

2.1.2 vse kontrole in sisteme v obsegu Sistema upravljanja informacijske varnosti (ISMS),

2.1.3 vse notranje revizije, preglede varnostnih kontrol in preverjanja skladnosti, ne glede na to, ali jih izvaja organizacija sama ali zunanji svetovalec, naročnik ali regulator.

2.2 Ta politika velja tudi za zbiranje dokazil in poročanje za:

2.2.1 certifikacijske in recertifikacijske presoje ISO/IEC 27001,

2.2.2 presoje varstva podatkov v skladu z GDPR ali pogodbenimi določili,

2.2.3 varnostne vprašalnike naročnikov ali preglede skrbnega pregleda,

2.2.4 vse regulativne ali neodvisne preglede v skladu z NIS2 ali DORA, kjer je to ustrezno.

3. Cilji

3.1 Zagotoviti, da se vse ključne kontrole in politike redno pregledujejo z vidika učinkovitosti in skladnosti.

3.2 Vzdrževati revizijsko sled ter evidence korektivnih ukrepov za izkazovanje odgovornosti in izboljševanja.

3.3 Pripraviti se na certifikacijo, recertifikacijo in programe zagotavljanja zaupanja naročnikov (npr. ISO 27001, vključevanje dobaviteljev).

3.4 Zgodaj prepoznati vrzeli, da se omogoči pravočasna odprava pred stopnjevanjem težav ali kršitvijo obveznosti.

3.5 Omogočiti generalnemu direktorju in izvajalcu IT usklajevanje pregledov z minimalno kompleksnostjo ob hkratnem zagotavljanju zagovorljivih rezultatov.

4. Vloge in odgovornosti

4.1 Generalni direktor (GM)

4.1.1 Nadzira program revizij.

4.1.2 Odobrava načrte notranjih pregledov in ugotovitve.

4.1.3 Dodeljuje korektivne ukrepe in spremlja njihovo izvedbo.

4.1.4 Odobri vključitev zunanjih revizorjev ali svetovalcev.

4.2 Izvajalec IT / skrbnik

4.2.1 Med notranjimi in zunanjimi revizijami zagotavlja dokazila (npr. dnevnike, konfiguracije, evidence o kontroli dostopa).

4.2.2 Sodeluje pri tehničnih preverjanjih (npr. stanje varnostnih kopij, skladnost nameščanja popravkov).

4.2.3 Vzdržuje repozitorij revizijskih dokazil.

[... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ...]

9. Zahteve za pregled in posodabljanje

9.1 Letni pregled politike in načrta revizij

9.1.1 Generalni direktor (GM) mora to politiko in razpored revizij pregledati najmanj enkrat letno.

9.1.2 V okviru pregleda je treba oceniti:

9.1.2.1 učinkovitost revizij pri prepoznavanju vrzeli,

9.1.2.2 stopnjo izvedbe revizij in korektivnih ukrepov,

9.1.2.3 spremembe veljavnih pravnih, regulativnih ali certifikacijskih zahtev.

9.2 Posodobitve na podlagi sprožilcev

9.2.1 Politiko je treba pregledati in posodobiti, kadar:

9.2.2 certifikacijska ali nadzorna revizija povzroči večjo neskladnost,

9.2.3 se spremenijo pravni ali regulativni okviri (npr. nova navodila GDPR, nacionalni prenos NIS2),

9.2.4 poslovne spremembe vplivajo na sisteme, procese ali dobavitelje, vključene v obseg revizije,

9.2.5 kritični incident ali kršitev razkrije predhodno neprepoznane vrzeli v kontrolah.

9.3 Dokumentiranje posodobitev

9.3.1 Vse spremembe se morajo evidentirati v evidenci verzij politike.

9.3.2 Posodobitve morajo biti posredovane vsem članom ekipe, ki sodelujejo pri revizijah.

9.3.3 Posodobljeni politiki mora biti priložen povzetek sprememb, da se zagotovi razumevanje.

10. Povezane politike in povezave

10.1 To politiko podpirajo in dopolnjujejo naslednje politike MSP:

10.1.1 P1S – Politika informacijske varnosti: določa izhodišča za vsa pričakovanja glede kontrol in zahteva njihovo preverjanje z revizijami.

10.1.2 P2S – Politika vlog in odgovornosti pri upravljanju: določa odgovornosti za načrtovanje revizij, izvedbo in lastništvo korektivnih ukrepov.

10.1.3 P6S – Politika upravljanja tveganj: opredeljuje pomanjkljivosti kontrol, odkrite pri revizijah, in zagotavlja, da so ugotovitve dokumentirane v registru tveganj.

10.1.4 P17S – Politika varstva podatkov in zasebnosti: določa kontrole GDPR, ki jih je treba revidirati, vključno z ravnanjem s podatki, odzivom na kršitve in obvestili o zasebnosti.

10.1.5 P22S – Politika beleženja in spremljanja: zagotavlja revizijske dnevnike in forenzične podatke, ki se uporabljajo pri pregledih skladnosti in kontrol.

10.1.6 P30S – Politika odzivanja na incidente: zahteva periodično revizijo evidenc incidentov in pregledov po dogodku za preverjanje učinkovitosti odzivanja.

10.1.7 P31S – Politika zbiranja dokazil in forenzike: določa postopke za zbiranje preverljivih dokazil z ohranjeno verigo skrbništva med revizijami.

10.2 Te politike skupaj vzpostavljajo celovito kontrolno okolje, ki omogoča notranje preverjanje, zunanje zagotavljanje zaupanja in upravljanje, usklajeno s standardi.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001:

11.1.1 Klavzula 9.2 – Zahteva notranje revizije za ocenjevanje delovanja ISMS in njegove skladnosti z zahtevami.

11.1.2 Klavzula 10.1 – Zahteva nenehno izboljševanje na podlagi rezultatov revizij in odprave neskladnosti.

11.2 ISO/IEC 27002:

11.2.1 Kontrola 5.35 – Zahteva načrtovane notranje preglede kontrol in procesov.

11.2.2 Kontrola 5.37 – Poudarja neodvisne preglede, zlasti za zunanje izvajane procese.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CA-2 – Varnostne presoje: zahteva revizije uvedenih kontrol za preverjanje njihove učinkovitosti.

11.3.2 CA-7 – Neprekinjeno spremljanje: poudarja proaktivno odkrivanje in pregled pomanjkljivosti kontrol.

11.3.3 AU-6 – Pregled, analiza in poročanje o revizijah: zahteva redno analizo in obravnavo revizijskih dnevnikov in ugotovitev.

11.4 Uredba EU GDPR:

11.4.1 Člena 24 in 32 – Zahtevata uvedbo in revidiranje tehničnih in organizacijskih ukrepov, vključno z dokazili o učinkovitosti kontrol in izboljševanjem skozi čas.

11.5 Direktiva EU NIS2 (2022/2555):

11.5.1 Člena 20–21 – Zahtevata proaktivni pregled kontrol, dokazljivo podprto skladnost in preverljivost za bistvene in pomembne subjekte.

11.6 COBIT 2019:

11.6.1 MEA01 – Spremljanje, vrednotenje in presoja uspešnosti ter skladnosti: zahteva periodično presojo uspešnosti procesov in kontrol glede na standarde in cilje.

11.6.2 MEA03 – Zagotavljanje skladnosti z zunanjimi zahtevami: osredotoča se na notranje spremljanje in pripravljenost na revizije tretjih oseb ter regulativne preglede.