					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P33S					Naziv dokumenta: **Politika revizijskog praćenja i usklađenosti**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađeno sa standardima i propisima

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točke 9.2, 10	Unutarnje revizije, kontinuirano poboljšavanje i otklanjanje nesukladnosti
ISO/IEC 27002:2022	Kontrole 5.35, 5.37	Planirani interni pregledi, neovisni pregledi izdvojenih procesa
NIST SP 800-53 Rev.5	CA-2, CA-7, AU-6	Sigurnosne procjene, kontinuirano praćenje, pregled/analiza/izvješćivanje o reviziji
GDPR EU	Članci 24 i 32	Revizija tehničkih i organizacijskih mjera, dokazi o djelotvornosti kontrola
Direktiva EU NIS2	Članak 21(2)(f)	Proaktivni pregled i usklađenost temeljena na dokazima
Uredba EU DORA	Članak 10	Upravljanje IKT rizicima, praćenje i izvješćivanje
COBIT 2019	MEA01, MEA03	Praćenje/procjena usklađenosti, spremnost za preglede trećih strana

1. Svrha

1.1 Ova politika uspostavlja pristup organizacije provedbi unutarnjih revizija, provjera sigurnosnih kontrola i praćenja usklađenosti s regulatornim zahtjevima. Njome se osigurava da sve kontrole, politike, sustavi i pružatelji usluga podliježu redovitom i strukturiranom pregledu.

1.2 Svrha ove politike jest otkrivanje neuspjeha kontrola, sprječavanje neusklađenosti i dokazivanje dužne pažnje u skladu s normom ISO/IEC 27001, GDPR-om i povezanim okvirima.

1.3 Ova politika malim i srednjim poduzećima omogućuje održavanje operativne kontrole i spremnosti za certifikaciju, čak i bez namjenskog odjela za usklađenost, primjenom jednostavnih, ponovljivih kontrolnih popisa i nalaza prioritiziranih prema riziku.

2. Područje primjene

2.1 Ova politika primjenjuje se na:

2.1.1 sve interne odjele i vanjske pružatelje usluga koji imaju odgovornosti povezane s IT sustavima, osobnim podacima i poslovno kritičnim uslugama

2.1.2 sve kontrole i sustave unutar opsega sustava upravljanja informacijskom sigurnošću (ISMS)

2.1.3 sve unutarnje revizije, preglede sigurnosnih kontrola i provjere usklađenosti, neovisno o tome provode li se interno ili ih provodi vanjski konzultant, klijent ili regulator

2.2 Ova politika također se primjenjuje na prikupljanje dokaza i izvješćivanje za:

2.2.1 certifikacijske i recertifikacijske revizije prema normi ISO/IEC 27001

2.2.2 revizije zaštite podataka prema GDPR-u ili ugovornim uvjetima

2.2.3 sigurnosne upitnike koje zahtijevaju klijenti ili postupke dubinske analize

2.2.4 sve regulatorne ili neovisne preglede prema NIS2 ili DORA-i, gdje je primjenjivo

3. Ciljevi

3.1 Osigurati da se sve ključne kontrole i politike redovito pregledavaju u pogledu djelotvornosti i usklađenosti.

3.2 Održavati revizijski trag i evidenciju korektivnih radnji radi dokazivanja odgovornosti i poboljšavanja.

3.3 Pripremiti organizaciju za certifikaciju, recertifikaciju i programe dokazivanja sigurnosti prema zahtjevima klijenata (npr. ISO 27001, uvođenje dobavljača).

3.4 Rano prepoznati nedostatke u kontrolama kako bi se omogućilo pravodobno otklanjanje prije nego što problemi eskaliraju ili dovedu do povrede obveza.

3.5 Omogućiti glavnom direktoru i pružatelju IT podrške koordinaciju pregleda uz minimalnu složenost, uz osiguravanje dokazivih ishoda.

4. Uloge i odgovornosti

4.1 Glavni direktor (GM)

4.1.1 nadzire program revizije

4.1.2 odobrava planove unutarnjih pregleda i nalaze

4.1.3 dodjeljuje i prati korektivne radnje

4.1.4 odobrava angažiranje vanjskih revizora ili konzultanata

4.2 Pružatelj IT podrške / administrator

4.2.1 osigurava dokaze tijekom unutarnjih i vanjskih revizija (npr. dnevničke zapise, konfiguracije, evidenciju kontrole pristupa)

4.2.2 pomaže u tehničkim provjerama (npr. status sigurnosnog kopiranja, usklađenost zakrpa)

4.2.3 održava repozitorij revizijskih dokaza

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Zahtjevi za pregled i ažuriranje

9.1 Godišnji pregled politike i plana revizije

9.1.1 Glavni direktor (GM) mora pregledati ovu politiku i raspored revizije najmanje jednom godišnje.

9.1.2 pregled mora obuhvatiti procjenu:

9.1.2.1 djelotvornosti revizija u utvrđivanju nedostataka u kontrolama

9.1.2.2 stope dovršenosti revizija i korektivnih radnji

9.1.2.3 promjena u primjenjivim pravnim, regulatornim ili certifikacijskim zahtjevima

9.2 Ažuriranja na temelju okidača

9.2.1 politika se mora pregledati i ažurirati kada:

9.2.2 certifikacijska ili nadzorna revizija rezultira većom nesukladnošću

9.2.3 promijene se pravni ili regulatorni okviri (npr. nove smjernice za GDPR, nacionalna provedba NIS2)

9.2.4 poslovne promjene utječu na sustave, procese ili dobavljače uključene u opseg revizije

9.2.5 kritični incident ili povreda otkriju prethodno neprepoznate nedostatke u kontrolama

9.3 Dokumentiranje ažuriranja

9.3.1 sve izmjene moraju se pratiti u zapisniku upravljanja verzijama politike

9.3.2 ažuriranja se moraju distribuirati svim članovima tima uključenima u revizije

9.3.3 uz ažuriranu politiku mora se priložiti sažetak promjena radi osiguravanja razumijevanja

10. Povezane politike i poveznice

10.1 Ovu politiku podupiru i dodatno osnažuju druge SME politike:

10.1.1 P1S – Politika informacijske sigurnosti: utvrđuje osnovu svih očekivanja u pogledu kontrola i zahtijeva njihovu provjeru putem revizija.

10.1.2 P2S – Politika uloga i odgovornosti u upravljanju: uspostavlja odgovornost za planiranje revizije, provedbu i vlasništvo nad korektivnim radnjama.

10.1.3 P6S – Politika upravljanja rizicima: utvrđuje slabosti kontrola otkrivene revizijama i osigurava da se nalazi dokumentiraju u registru rizika.

10.1.4 P17S – Politika zaštite podataka i privatnosti: definira GDPR kontrole koje se moraju revidirati, uključujući obradu podataka, odgovor na povrede i obavijesti o privatnosti.

10.1.5 P22S – Politika zapisivanja događaja i praćenja: osigurava revizijske dnevnike i forenzičke podatke koji se koriste tijekom pregleda usklađenosti i kontrola.

10.1.6 P30S – Politika odgovora na incidente: zahtijeva periodičnu reviziju zapisa o incidentima i pregleda nakon događaja radi provjere djelotvornosti odgovora.

10.1.7 P31S – Politika prikupljanja dokaza i forenzike: pruža postupke za prikupljanje provjerljivih dokaza uz lanac nadzora tijekom revizija.

10.2 Zajedno, ove politike uspostavljaju zatvoreno kontrolno okruženje koje omogućuje unutarnju provjeru, vanjsku potvrdu i upravljanje usklađeno sa standardima.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001:

11.1.1 Točka 9.2 – zahtijeva unutarnje revizije radi vrednovanja uspješnosti ISMS-a i njegove usklađenosti sa zahtjevima.

11.1.2 Točka 10.1 – zahtijeva kontinuirano poboljšavanje na temelju rezultata revizije i otklanjanja nesukladnosti.

11.2 ISO/IEC 27002:

11.2.1 Kontrola 5.35 – zahtijeva planirane interne preglede kontrola i procesa.

11.2.2 Kontrola 5.37 – naglašava neovisne preglede, osobito za izdvojene procese.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CA-2 – Sigurnosne procjene: zahtijeva revizije implementiranih kontrola radi provjere djelotvornosti.

11.3.2 CA-7 – Kontinuirano praćenje: naglašava proaktivno otkrivanje i pregled slabosti kontrola.

11.3.3 AU-6 – Pregled, analiza i izvješćivanje o reviziji: zahtijeva redovitu analizu i rješavanje revizijskih dnevničkih zapisa i nalaza.

11.4 GDPR EU:

11.4.1 Članci 24 i 32 – zahtijevaju provedbu i reviziju tehničkih i organizacijskih mjera, uključujući dokaze o djelotvornosti kontrola i poboljšavanju tijekom vremena.

11.5 Direktiva EU NIS2 (2022/2555):

11.5.1 Članci 20–21 – zahtijevaju proaktivni pregled kontrola, usklađenost temeljenu na dokazima i mogućnost provedbe revizije za ključne i važne subjekte.

11.6 COBIT 2019:

11.6.1 MEA01 – Praćenje, vrednovanje i procjena uspješnosti i usklađenosti: zahtijeva periodičnu procjenu uspješnosti procesa i kontrola u odnosu na standarde i ciljeve.

11.6.2 MEA03 – Osiguravanje usklađenosti s vanjskim zahtjevima: usmjereno je na interno praćenje i spremnost za revizije trećih strana i regulatorne preglede.