					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P01S					Naziv dokumenta: **Politika informacijske sigurnosti**							
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/propis	Točka/članak	Napomena
ISO/IEC 27001:2022	Točke 5.1, 5.2, 5.3, 6.1, 8	Propisuje opredijeljenost uprave, zahtjeve za politike, dodjelu uloga, procjenu rizika i operativne kontrole
ISO/IEC 27002:2022	Kontrole 5.1–5.5	Propisuje izradu dokumentiranih politika informacijske sigurnosti, dodjelu uloga, razdvajanje dužnosti i odgovornosti uprave
NIST SP 800-53 Rev.5	PM-1, PL-1, CA-1, AC-1	Zahtjevi za plan programa sigurnosti, politiku planiranja, procjenu/autorizaciju i kontrolu pristupa
GDPR EU (2016/679)	Članak 5. stavak 2., članak 32.	Načelo odgovornosti i sigurnost obrade, osobito u pogledu dokumentiranih uloga
Direktiva EU NIS2 (2022/2555)	Članak 21. stavak 2. točka (a)	Zahtijeva mjere upravljanja rizicima te definirane uloge i odgovornosti za kibernetički rizik
Uredba EU DORA (2022/2554)	Članak 9., članak 10.	Zahtijeva dodjelu uloga za upravljanje IKT rizikom i kontinuitet poslovanja
COBIT 2019	EDM03, APO13, DSS05	Osigurava optimizaciju rizika, upravljanje sigurnošću i upravljanje sigurnosnim uslugama putem jasne dodjele uloga

1. Svrha

1.1 Ova politika potvrđuje opredijeljenost organizacije zaštiti informacija o klijentima i poslovnih informacija jasnim definiranjem odgovornosti i primjenom praktičnih sigurnosnih mjera primjerenih organizacijama bez namjenskih IT timova.

1.2 Ovom politikom osigurava se da svi zaposlenici, ugovorni izvođači i pružatelji usluga postupaju u skladu s obvezujućim pravilima, čime se omogućuje potpuna usklađenost sa zahtjevima za certifikaciju prema normi ISO/IEC 27001.

1.3 Ova politika omogućuje organizaciji izgradnju povjerenja klijenata jasnim dokazivanjem načina na koji štitimo njihove informacije kroz definirane odgovornosti, strukturirane procese i jasno utvrđenu odgovornost.

2. Područje primjene

2.1 Ova politika primjenjuje se na sve osobe koje pristupaju podacima i sustavima organizacije ili njima upravljaju, uključujući:

2.1.1 vlasnike poslovanja i više rukovodstvo

2.1.2 zaposlenike, ugovorne izvođače i pripravnike

2.1.3 vanjske pružatelje IT usluga ili konzultante

2.2 Ova politika obuhvaća sve vrste informacija, sustava i usluga, uključujući:

2.2.1 poslovne evidencije, podatke o klijentima, lozinke i elektroničku poštu

2.2.2 IT opremu kao što su prijenosna računala i telefoni

2.2.3 usluge u oblaku koje se koriste za pohranu datoteka, komunikaciju ili financijske aktivnosti

2.2.4 fizičke dokumente pohranjene na lokacijama organizacije

2.3 Politika se primjenjuje u svim radnim okruženjima — u uredima, pri radu na daljinu i u okruženjima u oblaku — te obuhvaća sve uređaje i softver koji se koriste za obradu ili pohranu poslovnih informacija.

3. Ciljevi

3.1 Jasno dodijeliti odgovornost: osigurati da za informacijsku sigurnost uvijek bude određena odgovorna osoba. To je u pravilu glavni rukovoditelj ili osoba koju on formalno imenuje.

3.2 Zaštititi informacije o klijentima i poslovne informacije: uspostaviti pouzdane i dosljedne zaštitne mjere radi sprječavanja zlouporabe, gubitka ili krađe osjetljivih podataka, uključujući podatke o klijentima i financijsku dokumentaciju.

3.3 Podržati certifikaciju prema ISO/IEC 27001: omogućiti organizaciji dokazivanje potpune usklađenosti sa zahtjevima norme ISO/IEC 27001, uz spremnost za audit i ispunjavanje uvjeta za certifikaciju bez potrebe za složenom infrastrukturom.

3.4 Ugraditi sigurnost u poslovne aktivnosti: integrirati informacijsku sigurnost u svakodnevne zadatke i odluke u cijeloj organizaciji.

3.5 Izgraditi sigurnosnu svijest i kulturu: osigurati da svaki zaposlenik razumije i primjenjuje sigurnosne prakse, kao što su uporaba snažnih lozinki i prijavljivanje sumnjivih aktivnosti.

4. Uloge i odgovornosti

4.1 Glavni rukovoditelj ili vlasnik poslovanja

4.1.1 Snosi punu odgovornost za informacijsku sigurnost.

4.1.2 Odobrava i održava ovu politiku.

4.1.3 Osigurava da se svi ključni sigurnosni zadaci ili izvršavaju izravno ili formalno dodjeljuju u pisanom obliku.

4.1.4 Provjerava da se svi delegirani sigurnosni zadaci, kao što su upravljanje pristupom ili odgovor na incidente, provode učinkovito.

4.1.5 Djeluje kao zadana kontaktna osoba za sva interna i eksterna pitanja povezana sa sigurnošću, uključujući audite i upite klijenata.

4.1.6 Tijekom godišnjeg pregleda prati napredak u odnosu na ove ciljeve. Gdje je to moguće, ciljevi moraju biti mjerljivi (npr. % osposobljenog osoblja, broj prijavljenih incidenata i sl.) te se moraju revidirati na temelju sigurnosnih nalaza i promjena rizika.

4.2 Određeni zaposlenik (ako je primjenjivo)

4.2.1 Može pomagati glavnom rukovoditelju u upravljanju svakodnevnim zadacima, kao što su otvaranje korisničkih računa, ukidanje pristupnih prava zaposlenicima koji odlaze ili koordinacija s pružateljem IT usluga.

4.2.2 Mora biti službeno imenovan te imati dovoljno ovlasti i alata za izvršavanje zadataka.

4.2.3 Sve probleme prijavljuje glavnom rukovoditelju.

[... 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

9.1.1 Ovu politiku glavni rukovoditelj (GM) mora pregledati najmanje jednom godišnje kako bi se osigurala trajna usklađenost sa zahtjevima za certifikaciju prema normi ISO/IEC 27001, regulatornim promjenama (kao što su GDPR, NIS2 i DORA) i promjenjivim poslovnim potrebama.

9.2 Izvanredni pregledi

9.2.1 Dodatni pregledi moraju se provesti kad god nastupe značajne promjene, kao što su:

9.2.1.1 veliki sigurnosni incidenti ili povrede

9.2.1.2 uvođenje novih poslovnih procesa ili tehnologija (npr. novi softver, platforme za rad na daljinu ili usluge u oblaku)

9.2.1.3 promjene zakonskih ili regulatornih zahtjeva koje utječu na postupanje s informacijama

9.3 Dokumentiranje promjena

9.3.1 Svi pregledi politike i sve promjene moraju biti formalno dokumentirani, uz jasno navođenje datuma, prirode izmjena i odobrenja GM-a.

9.3.2 Povijest verzija politike mora se sigurno održavati kako bi se tijekom audita mogla dokazati evolucija politike i usklađenost.

9.4 Komunikacija ažuriranja

9.4.1 Sve promjene ove politike moraju se bez odgode priopćiti svim zaposlenicima, ugovornim izvođačima i relevantnim trećim stranama.

9.4.2 Ažurirane verzije politike moraju biti lako dostupne svom obuhvaćenom osoblju (npr. elektronički distribuirane ili fizički istaknute na radnom mjestu).

10. Povezane politike i poveznice

10.1 Ova je politika usko povezana s drugim politikama u skupu SME politika organizacije, a osobito sa sljedećima:

10.1.1 P2S – Politika uloga i odgovornosti upravljanja: pojašnjava dodjelu sigurnosnih dužnosti i odgovornosti.

10.1.2 P4S – Politika kontrole pristupa: definira sigurno upravljanje pristupom informacijama organizacije.

10.1.3 P8S – Politika podizanja svijesti i osposobljavanja o informacijskoj sigurnosti: pruža osnovne smjernice za osposobljavanje osoblja i podizanje svijesti.

10.1.4 P17S – Politika zaštite podataka i privatnosti: osigurava usklađenost s GDPR-om i drugim propisima o zaštiti podataka.

10.1.5 P30S – Politika upravljanja sigurnosnim incidentima: opisuje detaljne radnje potrebne kao odgovor na sigurnosne incidente.

10.2 Ove povezane politike pružaju jasne operativne smjernice i moraju se provoditi zajedno kako bi se postigla potpuna usklađenost sa zahtjevima certifikacije prema normi ISO/IEC 27001.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 5.1 – Vodstvo i opredijeljenost: zahtijeva opredijeljenost i odgovornost najvišeg rukovodstva za djelotvornost informacijske sigurnosti unutar organizacije.

11.1.2 Točka 5.2 – Politika informacijske sigurnosti: propisuje jasne, dokumentirane politike usklađene sa strategijom organizacije i zahtjevima usklađenosti.

11.1.3 Točka 5.3 – Organizacijske uloge i odgovornosti: definira jasnu dodjelu odgovornosti za informacijsku sigurnost u cijeloj organizaciji, što je ključno za učinkovito upravljanje i usklađenost tijekom audita.

11.1.4 Točka 6.1 – Radnje za rješavanje rizika i prilika: osigurava da se rizici informacijske sigurnosti sustavno identificiraju, vrednuju i obrađuju.

11.1.5 Točka 8.1 – Operativno planiranje i kontrola: zahtijeva da organizacija planira i provodi procese potrebne za ostvarenje ciljeva informacijske sigurnosti te učinkovito upravlja povezanim rizicima.

11.2 ISO/IEC 27002:2022 Kontrole 5.1–5.5

11.2.1 Dodatak A, kontrola 5.1 – Politike informacijske sigurnosti: propisuje izradu i komunikaciju dokumentiranih politika informacijske sigurnosti.

11.2.2 Dodatak A, kontrola 5.2 – Uloge informacijske sigurnosti: pojašnjava i formalno dodjeljuje uloge i odgovornosti za informacijsku sigurnost relevantnim stranama.

11.2.3 Dodatak A, kontrola 5.3 – Razdvajanje dužnosti: zahtijeva jasno razdvajanje dužnosti radi smanjenja sukoba interesa i rizika od prijevare pri upravljanju osjetljivim informacijama.

11.2.4 Dodatak A, kontrola 5.4 – Odgovornosti uprave: propisuje da uprava mora pokazati opredijeljenost za informacijsku sigurnost kroz aktivni nadzor i dodjelu resursa.

11.2.5 Ojačava potrebu za jasno dokumentiranim politikama informacijske sigurnosti, ulogama, odgovornostima i upravljačkim strukturama, čime se osigurava dosljedno upravljanje i sljedivost za potrebe audita u cijeloj organizaciji.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1 – Plan programa informacijske sigurnosti: zahtijeva dokumentirane strategije upravljanja informacijskom sigurnošću i politike koje predstavljaju okvir za dosljednu provedbu i upravljanje.

11.3.2 PL-1 – Politika sigurnosnog planiranja: propisuje sigurnosnu politiku na razini cijele organizacije kao smjernicu za siguran rad i strateško usklađivanje aktivnosti informacijske sigurnosti.

11.3.3 CA-1 – Politika procjene i autorizacije sigurnosti: zahtijeva jasno definirane uloge za procjenu i autorizaciju kako bi se osigurala trajna djelotvornost i usklađenost sa zahtjevima informacijske sigurnosti.

11.3.4 AC-1 – Politika kontrole pristupa: zahtijeva da organizacije jasno definiraju, dokumentiraju i provode prakse i odgovornosti upravljanja pristupom.

11.4 GDPR EU (2016/679)

11.4.1 Članak 5. stavak 2. – Načelo odgovornosti: zahtijeva da organizacije dokažu usklađenost s načelima zaštite podataka, uključujući dokumentirane uloge i politike za odgovornosti povezane sa zaštitom podataka.

11.4.2 Članak 32. – Sigurnost obrade: propisuje provedbu odgovarajućih tehničkih i organizacijskih mjera, uključujući jasno definirane sigurnosne odgovornosti, radi zaštite osobnih podataka od povreda i neovlaštenog pristupa.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Članak 21. stavak 2. točka (a) – Mjere upravljanja rizicima: zahtijeva jasna upravljačka uređenja, uključujući definirane uloge i odgovornosti za informacijsku sigurnost, što je nužno za učinkovito upravljanje kibernetičkim rizicima.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Članak 9. – Upravljanje IKT rizikom: zahtijeva da organizacije jasno dodijele uloge i odgovornosti povezane s upravljanjem IKT rizikom, čime se jača otpornost i spremnost za kontinuitet poslovanja.

11.6.2 Članak 10. – Kontinuitet poslovanja IKT-a: zahtijeva jasnu odgovornost i strukturirane uloge za održavanje otpornosti i kontinuiteta IKT-a, čime se osigurava da organizacije mogu pouzdano odgovoriti na poremećaje.

11.7 COBIT 2019

11.7.1 EDM03 – Osigurati optimizaciju rizika: naglašava jasno definiranu odgovornost i uloge u upravljanju organizacijskim rizicima te osigurava snažno upravljanje i učinkovit nadzor nad rizicima informacijske sigurnosti.

11.7.2 APO13 – Upravljati sigurnošću: zahtijeva da organizacije jasno uspostave i komuniciraju odgovornosti za upravljanje sigurnošću, osiguravajući usklađenost s poslovnim ciljevima i regulatornim zahtjevima.

11.7.3 DSS05 – Upravljati sigurnosnim uslugama: traži strukturirane uloge i jasne odgovornosti u upravljanju sigurnosnim uslugama, čime se omogućuju dosljedna provedba i provjera usklađenosti.