					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P01					Naslov dokumenta: **Politika informacijske varnosti**							
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**

1. Namen

1.1 Ta politika opredeljuje krovno zavezanost organizacije k informacijski varnosti z vzpostavitvijo formalnega sistema upravljanja informacijske varnosti (ISMS).

1.2 Določa strateško usmeritev in temeljne zahteve za varovanje zaupnosti, celovitosti, razpoložljivosti in odpornosti vseh informacijskih sredstev v fizičnih, digitalnih in oblačnih okoljih.

1.3 Politika izpolnjuje zahteve klavzul 5.2 in 5.1 standarda ISO/IEC 27001:2022, saj izraža namen vodstva, zavezanost najvišjega vodstva in usklajenost varnostnih dejavnosti s cilji organizacije.

1.4 Predstavlja avtoritativno referenco za vse podrejene politike, standarde in postopke v okviru ISMS ter je bistvena za vzpostavitev varnostnega okolja, ki temelji na tveganjih, skladnosti in nenehnem izboljševanju.

2. Obseg

2.1 Ta politika velja za vse posameznike, sredstva in procese, opredeljene v obsegu ISMS, vključno z:

2.1.1 vsemi poslovnimi enotami, oddelki, odvisnimi družbami in podružnicami,

2.1.2 zaposlenimi, pogodbenimi izvajalci, začasnimi delavci, svetovalci in ponudniki storitev tretjih oseb,

2.1.3 vsemi podatki, informacijskimi sistemi, aplikacijami, infrastrukturo in komunikacijskimi kanali,

2.1.4 vsemi fizičnimi, oblačnimi, oddaljenimi in hibridnimi okolji, v katerih se obdelujejo podatki podjetja ali se do njih dostopa.

2.2 Politika je zavezujoča za vse subjekte, ki obdelujejo informacije organizacije, in velja za vse faze življenjskega cikla informacij, od nastanka in prenosa do hrambe in uničenja.

2.3 Vse izključitve ali omejitve tega obsega morajo biti dokumentirane v izjavi o obsegu ISMS in utemeljene s formalno odobritvijo najvišjega vodstva.

3. Cilji

3.1 Vzpostaviti ISMS, ki je skladen z ISO/IEC 27001:2022 in podpira odločanje na podlagi tveganj v celotni organizaciji.

3.2 Zagotoviti, da so načela zaupnosti, celovitosti in razpoložljivosti vključena v vse dejavnosti, sisteme in partnerstva organizacije.

3.3 Omogočiti regulativno in pogodbeno skladnost z opredelitvijo merljivih varnostnih ciljev, ki izhajajo iz te politike, ter njihovo vključitvijo v poslovanje.

3.4 Zmanjšati verjetnost in vpliv incidentov informacijske varnosti z učinkovitimi preventivnimi, detektivnimi in korektivnimi kontrolami.

3.5 Spodbujati nenehno izboljševanje zrelosti informacijske varnosti z opredeljenimi kazalniki uspešnosti, rezultati presoj in vodstvenimi pregledi.

3.6 Krepiti kulturo odgovornosti, ozaveščenosti in odpornosti, v kateri vsi zaposleni razumejo svoje varnostne odgovornosti in jih tudi izvajajo.

4. Vloge in odgovornosti

4.1 Najvišje vodstvo

4.1.1 Odobri in potrdi Politiko informacijske varnosti ter okvir ISMS.

4.1.2 Zagotavlja usklajenost med varnostnimi cilji in poslovno strategijo.

4.1.3 Daje zgled in spodbuja močno kulturo informacijske varnosti.

4.1.4 Pregleduje in odobrava večje spremembe obsega ISMS, obravnave tveganj in upravljavske strukture.

4.2 Vodja informacijske varnosti (CISO) / vodja ISMS

4.2.1 Odgovoren je za ISMS in vzdržuje to politiko v skladu z ISO/IEC 27001.

4.2.2 Vodi ocenjevanje tveganj, izvajanje kontrol in procese nenehnega izboljševanja.

4.2.3 Zagotavlja medfunkcijsko usklajevanje varnostnih dejavnosti in nadzira podrejene politike.

4.2.4 Izvršnemu vodstvu poroča o stanju ISMS, incidentih, rezultatih presoj in kazalnikih.

4.2.5 Zagotavlja, da se pregledi in posodobitve politike izvajajo v skladu z oddelkom 9 tega dokumenta.

[... 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 Pogostost pregledov

9.1.1 Ta politika se mora pregledati najmanj enkrat letno ali ob katerem koli od naslednjih sprožilcev:

9.1.1.1 pomembne spremembe pravnih, regulativnih ali pogodbenih obveznosti,

9.1.1.2 bistvene spremembe profila tveganja organizacije,

9.1.1.3 rezultati notranjih ali zunanjih presoj,

9.1.1.4 večji incidenti ali odpovedi kontrol.

9.2 Pristojnost in postopek pregleda

9.2.1 Postopek pregleda vodi vodja informacijske varnosti ali imenovani vodja ISMS.

9.2.2 Vhodni podatki za pregled morajo vključevati:

9.2.2.1 rezultate notranje revizije,

9.2.2.2 trende ocen tveganj,

9.2.2.3 spremembe poslovnih procesov in tehnologije,

9.2.2.4 uspešnost glede na ključne kazalnike uspešnosti (KPI) in pragove tveganja.

9.2.3 Vse posodobitve morajo:

9.2.3.1 biti verzionirane in dokumentirane,

9.2.3.2 biti odobrene s strani izvršnega vodstva,

9.2.3.3 biti posredovane vsem zadevnim stranem prek uradnih komunikacijskih kanalov,

9.2.3.4 sprožiti potrebne posodobitve podrejene dokumentacije in usposabljanj.

10. Povezane politike in povezave

10.1 Ta temeljna politika je neposredno povezana z naslednjimi organizacijskimi varnostnimi politikami in okviri:

10.1.1 P2 – Politika vlog in odgovornosti upravljanja: opredeljuje strukturo upravljanja in hierarhijo pooblastil, navedeno v tem dokumentu.

10.1.2 P3 – Politika sprejemljive uporabe (AUP): določa zahteve glede ustreznega ravnanja in skladnega vedenja pri uporabi informacijskih sredstev.

10.1.3 P4 – Politika nadzora dostopa: operativno uvaja kontrole, povezane z dostopom, ki izhajajo iz te krovne politike.

10.1.4 P6 – Politika obvladovanja tveganj: določa okvir na podlagi tveganj za izbiro kontrol in sprejem preostalega tveganja.

10.1.5 P33 – Politika spremljanja presoj in skladnosti: določa, kako notranji mehanizmi zagotovila potrjujejo izvajanje politike.

10.2 Te medsebojne odvisnosti zagotavljajo celovito usklajenost in sledljivost v okviru ISMS ter podpirajo enotno upravljanje tveganj in skladnosti.

11. Referenčni standardi in okviri

11.1 Ta Politika informacijske varnosti je formalno usklajena z naslednjimi standardi in okviri, da se zagotovijo popolna skladnost, pripravljenost na revizijo in regulatorna odgovornost:

11.2 ISO/IEC 27001

11.2.1 Klavzula 5.1 – Vodenje in zavezanost: ta politika izkazuje zavezanost najvišjega vodstva informacijski varnosti ter določa odgovornosti in dodelitev virov za ISMS.

11.2.2 Klavzula 5.2 – Politika informacijske varnosti: ta dokument predstavlja formalno varnostno politiko organizacije, usklajeno z opredeljenimi varnostnimi cilji, poslovno strategijo in skladnostjo z ISO/IEC 27001.

11.2.3 Klavzula 6.1 – Ukrepi za obravnavo tveganj in priložnosti: pristop na podlagi tveganj, kot je opredeljen v tej politiki, zagotavlja, da se varnostni viri uporabljajo sorazmerno glede na grožnje.

11.2.4 Klavzula 9.2 – Notranja revizija in klavzula 10 – Izboljševanje: ta politika je vključena v cikel nenehnega izboljševanja organizacije in je predmet preverjanja v okviru notranje revizije.

11.2.5 ISO/IEC 27002:2022 – Kontrola 5.1: določa smernice za vzpostavitev in vzdrževanje varnostnih politik. Ta politika sledi priporočilom standarda ISO/IEC 27002 glede hierarhične dokumentacije, ciklov pregledov in možnosti uveljavljanja.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 (Politika in postopki varnostnega načrtovanja): ta politika izpolnjuje zahtevo po pripravi, razširjanju in pregledu formalne politike informacijske varnosti na ravni celotne organizacije.

11.3.2 PM-1 do PM-5: obravnava upravljanje na ravni programa, vključno z vlogami na področju informacijske varnosti, dodeljevanjem virov, strategijo tveganj in vključevanjem varnostnega načrtovanja v poslovanje organizacije.

11.4 Uredba EU GDPR (2016/679)

11.4.1 Člen 5(2): uveljavlja načelo odgovornosti. Ta politika določa odgovorne osebe in sledljive izvedbene ukrepe.

11.4.2 Člen 24: zahteva izvajanje tehničnih in organizacijskih ukrepov, vključno s politikami, usklajenimi s tveganji.

11.4.3 Člen 32: podpira izvajanje ustreznih ukrepov za zagotavljanje varnosti osebnih podatkov v celotnem njihovem življenjskem ciklu.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Člen 21(2)(a): subjektom nalaga uvedbo dokumentirane varnostne politike, ki obravnava obvladovanje tveganj in upravljanje. Ta politika izpolnjuje to zahtevo ter podpira širšo pripravljenost na kibernetsko varnost in zaščito kritične infrastrukture.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Člen 5(2): zahteva dokumentiran okvir notranjih kontrol za upravljanje tveganj IKT. Ta politika podpira skladnost finančnega sektorja z dodelitvijo vlog, kontrol in nadzornih funkcij, usklajenih s pričakovanji upravljanja iz Uredbe DORA.

11.7 COBIT 2019

11.7.1 EDM01 – Določitev okvira upravljanja: ta politika podpira korporativno upravljanje z določitvijo vlog ISMS, zavez vodstva in strateških ciljev.

11.7.2 APO01 – Okvir upravljanja: podpira vzpostavitev in delovanje strukturiranega ISMS.

11.7.3 APO12 – Obvladovanje tveganj: zagotavlja temelje za upravljanje tveganj informacijske varnosti.

11.7.4 MEA01/MEA03 – Spremljanje, vrednotenje in ocenjevanje: krepi stalno vrednotenje uspešnosti in spremljanje notranjih kontrol z uveljavljanjem skladnosti s politiko.