					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P13					Naslov dokumenta: **Politika razvrščanja in označevanja podatkov**							
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 določa formalni okvir za razvrščanje in označevanje informacijskih sredstev organizacije glede na občutljivost, izpostavljenost tveganjem in regulativne obveznosti.

1.2 Zagotavlja, da so vse informacije – ne glede na to, ali se shranjujejo, prenašajo ali obdelujejo – jasno kategorizirane in označene na način, ki izraža zahtevano raven zaščite in ravnanja.

1.3 Politika zahteva strukturirano razvrščanje, usklajeno s praksami organizacije na področju obvladovanja tveganj, ter podpira cilje zaupnosti, celovitosti in razpoložljivosti (CIA) pri digitalnih in fizičnih vrstah podatkov.

1.4 Ta kontrola je bistvena za omogočanje dostopa na podlagi vlog, pripravljenost na presojo, ustrezno izmenjavo podatkov in učinkovito uvedbo tehničnih varoval, kot so šifriranje, varnostno kopiranje in spremljanje.

2. Področje uporabe

2.1 Ta politika se uporablja za:

2.1.1 vsa informacijska sredstva organizacije, vključno z dokumenti, podatkovnimi zbirkami, evidencami in komunikacijami,

2.1.2 vse oblike podatkov, vključno z digitalnimi, tiskanimi, pisanimi ali ustnimi,

2.1.3 vsa okolja: v prostorih organizacije, oddaljena, mobilna in oblačna,

2.1.4 vse zaposlene, pogodbene izvajalce, ponudnike storitev in tretje osebe, ki obdelujejo podatke ter ustvarjajo, obravnavajo ali hranijo informacije organizacije.

2.2 Področje uporabe vključuje interno razvite vsebine, zunanje pridobljene podatke, osebne podatke, za katere veljajo obveznosti po zakonodaji o varstvu osebnih podatkov (npr. GDPR), ter informacije, izmenjane s strankami, partnerji in regulatorji.

2.3 Uporablja se za vse sisteme, ki se uporabljajo za shranjevanje ali prenos podatkov, vključno s poslovnimi aplikacijami, datotečnimi strežniki, e-poštnimi sistemi, oblačnimi platformami in repozitoriji varnostnih kopij.

3. Cilji

3.1 Vzpostaviti standardizirano shemo razvrščanja na ravni celotne organizacije na podlagi vpliva razkritja ali kompromitiranja podatkov.

3.2 Zagotoviti, da so vse informacije vidno in trajno označene tako, da odražajo svojo raven razvrstitve in zahteve glede ravnanja.

3.3 Uveljaviti kontrole ravnanja s podatki in nadzora dostopa, usklajene z razvrstitvijo, vključno s šifriranjem, beleženjem dnevnikov, zaščito prenosa in določitvijo rokov hrambe.

3.4 Podpirati skladnost z mednarodnimi standardi (ISO/IEC 27001, 27002), pravnimi okviri (GDPR, NIS2, DORA) in internimi politikami obvladovanja tveganj.

3.5 Zagotoviti, da vsi uporabniki razumejo svoje odgovornosti pri zaščiti podatkov, uporabi oznak in pravilnem ravnanju z razvrščenimi informacijami.

3.6 Ohranjati sledljivost med statusom razvrstitve, povezanimi kontrolami in popisom sredstev organizacije za namene presoje in skladnosti.

4. Vloge in odgovornosti

4.1 Vodja informacijske varnosti (CISO)

4.1.1 Je lastnik politike razvrščanja in označevanja informacij ter zagotavlja njeno usklajenost z regulativnimi, pogodbenimi in operativnimi zahtevami.

4.1.2 Odobri ravni razvrščanja, standarde označevanja in spremembe politike.

4.1.3 Nadzira skladnost s politiko prek presoj, kazalnikov in pregledov izjem.

4.1.4 Usklajuje medfunkcijsko upravljanje s pravno službo, funkcijo varstva podatkov in ekipami za obvladovanje tveganj.

4.2 Lastniki informacij

4.2.1 So odgovorni za razvrščanje informacijskih sredstev pod njihovim nadzorom z uporabo organizacijske sheme razvrščanja.

4.2.2 Oznake razvrstitve uporabijo ob nastanku, posodobitvi ali prevzemu informacij.

4.2.3 Redno pregledujejo razvrstitev sredstev, zlasti ob spremembah občutljivosti, regulativnega obsega ali poslovne vrednosti.

4.2.4 Zagotavljajo, da se z občutljivimi podatki ustrezno ravna in da so pravilno označeni skozi celoten življenjski cikel.

[... 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 Ta politika se mora pregledati najmanj enkrat letno, da se zagotovi usklajenost z:

9.1.1 spreminjajočimi se regulativnimi zahtevami (npr. GDPR, NIS2, DORA),

9.1.2 posodobitvami smernic ISO/IEC 27001 ali 27002 glede razvrščanja,

9.1.3 organizacijskimi spremembami, ki vplivajo na občutljivost podatkov ali lastništvo,

9.1.4 tehnološkimi spremembami, vključno z novimi platformami za upravljanje dokumentov ali podatkov.

9.2 Vodja informacijske varnosti (CISO) začne pregled v sodelovanju z odborom za informacijsko varnost, pravno službo in zadevnimi poslovnimi enotami.

9.3 Pregledi morajo vključevati:

9.3.1 učinkovitost uveljavljanja razvrščanja in stopnjo upoštevanja zahtev s strani uporabnikov,

9.3.2 analizo incidentov ali izjem, povezanih z napačno razvrstitvijo,

9.3.3 povratne informacije uporabnikov o orodjih za označevanje ali usmeritvenih gradivih,

9.3.4 primerjalno analizo s panožnimi standardi razvrščanja.

9.4 Posodobitve politike morajo biti ustrezno verzionirane, dokumentirane v repozitoriju ISMS in sporočene vsem ustreznim osebam s poudarkom na novih odgovornostih ali spremembah orodij.

9.5 Novi zaposleni morajo biti s trenutno različico politike seznanjeni med uvajanjem. Vsi zaposleni morajo po pomembnih spremembah politike opraviti obnovitveno usposabljanje.

10. Povezane politike in povezave

10.1 To politiko neposredno podpirajo in uveljavljajo kontrole, opisane v naslednjih povezanih politikah:

10.1.1 P4 - Politika nadzora dostopa: dostop do informacij se upravlja glede na ravni razvrščanja; občutljivejši podatki zahtevajo strožji nadzor dostopa in mehanizme odobritve.

10.1.2 P11 - Politika upravljanja uporabniških računov in privilegijev: krepi dodeljevanje privilegijev na podlagi potrebe po seznanitvi, kot jo določajo ravni razvrščanja.

10.1.3 P12 - Politika upravljanja sredstev: zagotavlja, da vsako sredstvo v popisu vključuje svojo razvrstitev in oznako, s čimer podpira sledljivost in odgovornost.

10.1.4 P14 - Politika hrambe in odstranjevanja podatkov: pravila odstranjevanja in hrambe se določajo glede na raven razvrstitve podatkov in regulativne zahteve glede hrambe.

10.1.5 P18 - Politika kriptografskih kontrol: uporablja ustrezne standarde šifriranja glede na razvrstitev informacijskega sredstva.

10.1.6 P22 - Politika beleženja dnevnikov in spremljanja: omogoča spremljanje dostopa do razvrščenih informacij in njihovega premikanja, s čimer zagotavlja revizijsko sled ter zaznavanje napačnega označevanja ali neprimerne uporabe.

10.2 Vsaka povezava zagotavlja dosledno zaščito informacij skozi njihov življenjski cikel, od nastanka in razvrščanja do varnega ravnanja, shranjevanja, prenosa in končnega uničenja.

11. Referenčni standardi in okviri

11.1 Ta politika je usklajena z mednarodno priznanimi standardi in regulativnimi okviri, ki urejajo razvrščanje in označevanje občutljivih informacij.

11.2 ISO/IEC 27001

11.2.1 Klavzula 4.2 - Razumevanje potreb in pričakovanj zainteresiranih strani. Zahteve glede razvrščanja pogosto izhajajo iz pravnih, regulativnih ali pogodbenih obveznosti, ki jih določajo zainteresirane strani (npr. GDPR, pogodba o nerazkrivanju informacij s stranko), in morajo biti odražene v tej politiki.

11.2.2 Klavzula 6.1.3 - Obravnava tveganj informacijske varnosti. Razvrščanje neposredno vpliva na izbiro kontrol za obravnavo tveganj, vključno z nadzorom dostopa, šifriranjem in hrambo, glede na občutljivost podatkov.

11.2.3 Klavzula 7.2 - Kompetentnost. Ta politika zahteva, da je osebje, odgovorno za razvrščanje in označevanje, usposobljeno, kar sodi med zahteve glede kompetentnosti.

11.2.4 Klavzula 7.3 - Ozaveščenost. Ta politika zahteva, da so vsi uporabniki seznanjeni z ravnmi razvrščanja in svojimi odgovornostmi pri ravnanju z informacijami, kar je usklajeno z obveznostmi glede ozaveščenosti.

11.2.5 Klavzula 7.5 - Dokumentirane informacije. Sama politika razvrščanja je nadzorovan dokument, postopki, evidence o usposabljanju in oznake razvrščanja pa so del dokumentiranih informacij.

11.2.6 Klavzula 8.1 - Operativno načrtovanje in nadzor. Razvrščanje in označevanje sta operativna procesa, vključena v upravljanje življenjskega cikla podatkov, ta klavzula pa zagotavlja, da so takšne dejavnosti načrtovane, izvedene in nadzorovane.

11.2.7 Klavzula 9.1 - Spremljanje, merjenje, analiza in vrednotenje. Politika vključuje določbe za spremljanje skladnosti razvrščanja, trendov incidentov in učinkovitosti sheme označevanja.

11.2.8 Klavzula 10.1 - Neskladnost in korektivni ukrep. Politika določa odzive na napačno razvrstitev, vključno s korektivnimi ukrepi, kot so ponovno usposabljanje, posodobitve in obravnava izjem.

11.3 ISO/IEC 27002:2022

11.3.1 Kontrola 5.12 - Razvrščanje informacij. Ta kontrola zagotavlja, da so informacije razvrščene glede na občutljivost, vrednost in kritičnost, kar ta politika formalno določa.

11.3.2 Kontrola 5.13 - Označevanje informacij. Ta kontrola zahteva ustrezno označevanje informacij v skladu z njihovo ravnjo razvrstitve, kar politika v celoti ureja.

11.3.3 Kontrola 5.10 - Sprejemljiva uporaba informacij in drugih povezanih sredstev. Ta politika določa, kako morajo uporabniki ravnati z razvrščenimi podatki, s čimer neposredno podpira sprejemljivo uporabo in preprečuje neustrezno uporabo.

11.3.4 Kontrola 5.11 - Vračilo sredstev. Razvrščanje pomaga zagotoviti, da so občutljivi podatki prepoznani ter varno vrnjeni ali sanirani, ko zaposleni ali dobavitelj preneha sodelovati z organizacijo.

11.3.5 Kontrola 5.9 - Popis informacij in drugih povezanih sredstev. Razvrščanje je pogosto povezano s popisom sredstev, ki mora odražati raven razvrstitve vsake postavke, da podpira pravilno dodelitev kontrol.

11.3.6 Kontrola 5.14 - Prenos informacij. Ravni razvrščanja vplivajo na kontrole pri internih in zunanjih prenosih podatkov (npr. šifriranje, odobritev, omejitve dostopa).

11.3.7 Kontrola 8.12 - Preprečevanje uhajanja podatkov. Uveljavljanje razvrščanja in označevanja podpira preprečevanje nepooblaščenega razkritja in izgube podatkov.

11.3.8 Kontrola 8.11 - Maskiranje podatkov. Nekatere ravni razvrščanja (npr. zaupno, omejeno) lahko zahtevajo maskiranje, kadar se podatki uporabljajo v testnih, razvojnih ali analitičnih okoljih.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-2 - Politika in postopki zaščite sistemov in komunikacij: podpira politike razvrščanja kot del krovnega varstva podatkov.

11.4.2 AC-16 - Varnostni atributi: omogoča uveljavljanje dostopa na podlagi metapodatkov razvrščanja in dovoljenj uporabnikov.

11.4.3 MP-3 / MP-5 - Označevanje nosilcev in zaščita pri transportu: uveljavlja označevanje in zaščito podatkov v mirovanju in med prenosom glede na razvrstitev.

11.5 Uredba EU GDPR (2016/679)

11.5.1 Člen 5 - Načela varstva podatkov: zahteva, da se osebni podatki obdelujejo varno in sorazmerno glede na njihovo občutljivost.

11.5.2 Člen 32 - Varnost obdelave: krepi razvrščanje kot mehanizem za varstvo podatkov na podlagi tveganja in uporabo ustreznih tehničnih ukrepov.

11.6 Direktiva EU NIS2 (2022/2555)

11.6.1 Člen 21(2)(a): zahteva politike za obvladovanje tveganj informacijske varnosti, vključno s kontrolami razvrščanja sredstev in podatkov.

11.6.2 Člen 21(3): spodbuja sprejetje ukrepov za uveljavljanje ustreznega ravnanja s podatki, kar podpira označevanje na podlagi razvrščanja.

11.7 Uredba EU DORA (2022/2554)

11.7.1 Člen 5 - Upravljanje in nadzor: zahteva okvire upravljanja, ki razvrščajo podatkovna sredstva za nadzor tveganj IKT.

11.7.2 Člen 9 - Upravljanje tveganj IKT: nalaga tehnične in organizacijske ukrepe za kritična sredstva IKT, vključno z razvrščanjem in označevanjem.

11.8 COBIT 2019

11.8.1 DSS05.02 - Upravljanje varnostnih storitev: uveljavlja razvrščanje informacijske varnosti za zagotavljanje zaščite podatkov organizacije.

11.8.2 MEA03 - Spremljanje, vrednotenje in ocenjevanje skladnosti: podpira redno revizijo in pregled praks razvrščanja za zagotavljanje skladnosti s politiko in zrelosti.