					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P13S					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**

Usklajeno s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
ISO/IEC 27001:2022	Klavzuli 5.3, 8	
ISO/IEC 27002:2022	Kontroli 5.12, 5.13	
NIST SP 800-53 Rev.5	AC-16, MP-3, MP-5	
Direktiva EU NIS2	Člen 21(2)(a)	
Uredba EU DORA	Člen 5(8)	
COBIT 2019	BAI03.05, DSS05	
Uredba EU GDPR	Člena 5, 32	

1. Namen

1.1 Ta politika določa, kako morajo biti vse informacije, ki jih organizacija obdeluje, razvrščene in označene, da se skozi njihov celoten življenjski cikel ohranjajo zaupnost, celovitost in razpoložljivost (CIA).

1.2 Omogoča dosledno ravnanje s podatki z dodelitvijo ustreznih ravni zaščite informacijam glede na njihovo občutljivost, poslovni vpliv ali pravne obveznosti.

1.3 Razvrščanje in označevanje pripomoreta k zmanjševanju tveganja nenamernega razkritja, nepooblaščenega dostopa ali neustreznega ravnanja z občutljivimi podatki, zlasti v malih in srednjih podjetjih, ki se lahko opirajo na enostavnejše sisteme in manj formalizirane kontrole.

1.4 Ta politika je ključna za certificiranje po ISO/IEC 27001 in regulatorno skladnost, zlasti z zakonodajo s področja varstva podatkov, kot je Uredba EU GDPR, ter okviri kibernetske varnosti, kot sta Direktiva EU NIS2 in Uredba EU DORA.

2. Področje uporabe

2.1 Ta politika velja za vse podatke organizacije ne glede na njihovo obliko ali lokacijo, vključno z:

2.1.1 elektronskimi dokumenti, preglednicami, elektronsko pošto, obrazci, slikami in skeniranimi datotekami;

2.1.2 fizičnimi dokumenti, kot so tiskani zapisi, poročila, računi in zapiski;

2.1.3 podatki, shranjenimi ali obdelovanimi v storitvah v oblaku, na lokalnih strežnikih, izmenljivih medijih ali napravah v osebni lasti, ki se uporabljajo za poslovne namene;

2.1.4 začasnimi ali prehodnimi podatki, ki nastajajo med poslovanjem (npr. dnevniki, predpomnilniške datoteke, elektronska pošta).

2.2 Vsi zaposleni, pogodbeni izvajalci, začasni delavci in zunanji ponudniki z dostopom do podatkov organizacije morajo upoštevati to politiko.

2.3 Politika velja skozi celoten življenjski cikel podatkov – od ustvarjanja in hrambe prek dostopa in prenosa do arhiviranja ali izbrisa.

3. Cilji

3.1 Določiti enostavno in izvršljivo shemo razvrščanja, ki jo je mogoče enotno razumeti in uporabljati v celotni organizaciji.

3.2 Zahtevati, da je vsak podatkovni vir razvrščen glede na svojo občutljivost in ustrezno označen, da se zagotovi pravilno ravnanje, hramba in dostop.

3.3 Zagotoviti, da so prakse označevanja podatkov vključene v poslovne delovne tokove, kot so uvajanje, zagon projektov in vzpostavitev sistemov.

3.4 Zmanjšati tveganje kršitev varnosti osebnih podatkov z uporabo kontrol ravnanja (npr. šifriranje, omejitev dostopa) glede na raven razvrstitve.

3.5 Zagotoviti skladnost z zakonodajo s področja zasebnosti in informacijske varnosti z izkazovanjem, da so občutljivi podatki (npr. osebni, finančni ali lastniški) ustrezno označeni in upravljani.

3.6 Vzpostaviti odgovornost za odločitve o razvrščanju ter zagotoviti periodične preglede in posodobitve glede na spreminjajoče se poslovne in pravne potrebe.

4. Vloge in odgovornosti

4.1 Generalni direktor (GM)

4.1.1 Je lastnik te politike in odobri shemo razvrščanja.

4.1.2 Zagotavlja nadzor nad tem, da so odgovornosti za razvrščanje ustrezno dodeljene in da se politika izvaja.

4.1.3 Pregleda in odobri vse izjeme od zahtev glede razvrščanja ali označevanja.

4.1.4 Zagotavlja, da prakse ravnanja s podatki izpolnjujejo zahteve glede skladnosti z zakonodajo, kot sta Uredba EU GDPR in Uredba EU DORA.

4.2 Lastnik informacij / upravljavec podatkov

4.2.1 Ob nastanku ali pridobitvi vsakemu novemu naboru podatkov ali informacijskemu sredstvu dodeli začetno razvrstitev.

4.2.2 Zagotavlja uporabo vidnih oznak, kjer je to ustrezno (npr. glave dokumentov, noge dokumentov, vodni žigi, imena map).

4.2.3 Periodično pregleduje razvrstitve, da preveri njihovo ustreznost, točnost in potrebo po spremembah (npr. po znižanju stopnje zaščite ali objavi).

4.2.4 Sodeluje z vodjo IT pri uvedbi tehničnih zaščitnih ukrepov na podlagi razvrstitve (npr. pravice dostopa, šifriranje).

[... 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 To politiko morata generalni direktor in upravljavec podatkov pregledati letno, da zagotovita, da odraža:

9.1.1 spremembe poslovanja ali vrst podatkov;

9.1.2 nove regulatorne zahteve (npr. glede zasebnosti podatkov ali finančnega nadzora);

9.1.3 tehnološke spremembe, ki vplivajo na zmožnosti označevanja ali razvrščanja.

9.2 Pregled mora vključevati posodobitve kategorij razvrščanja, orodij ali praks označevanja ter vsebin ozaveščanja in usposabljanja.

9.3 Revizije politike mora odobriti generalni direktor, o njih pa morajo biti obveščeni vsi zaposleni. Evidenca sprememb različic se mora hraniti za potrebe revizije.

10. Povezane politike in povezave

10.1 P2S – Politika vlog in odgovornosti upravljanja: določa odgovornost za lastništvo politike in njeno uveljavljanje.

10.2 P4S – Politika nadzora dostopa: usklajuje dostop do sistemov z ravnmi razvrstitve podatkov.

10.3 P12S – Politika upravljanja sredstev: spremlja fizična in digitalna sredstva, na katerih so shranjeni razvrščeni podatki.

10.4 P17S – Politika varstva podatkov in zasebnosti: ureja varstvo osebnih podatkov, od katerih je velik del razvrščen kot zaupno.

10.5 P30S – Politika odzivanja na incidente: določa eskalacijske poti in postopke odziva v primeru kršitev razvrščanja ali razkritja podatkov.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 5.3: zahteva jasno opredeljene odgovornosti za ravnanje s podatki in njihovo zaščito.

11.1.2 Klavzula 8.1: zahteva operativno načrtovanje in kontrole, vključno s tistimi, ki so povezane z razvrščanjem podatkov.

11.2 ISO/IEC 27002

11.2.1 Kontrola 5.12: podaja usmeritve za razvrščanje informacij na podlagi tveganj in regulatornih zahtev.

11.2.2 Kontrola 5.13: opisuje praktične mehanizme označevanja in povezana pravila ravnanja.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-16: zahteva označevanje informacij, da so zaščitni ukrepi usklajeni z razvrstitvijo.

11.3.2 MP-3 / MP-5: podajata usmeritve za označevanje in nadzor medijev ter izhodov.

11.4 Uredba EU GDPR

11.4.1 Člena 5 in 32: zahtevata minimizacijo podatkov ter celovitost z ustreznim razvrščanjem in zaščitnimi ukrepi pri ravnanju.

11.5 Direktiva EU NIS2

11.5.1 Člen 21(2)(a): zahteva tehnične in organizacijske kontrole za varstvo podatkov na podlagi tveganj.

11.6 Uredba EU DORA

11.6.1 Člen 5(8): zahteva, da podjetja razvrstijo podatkovna sredstva kot del programa upravljanja tveganj IKT.

11.7 COBIT 2019

11.7.1 BAI03.05: zahteva razvrščanje informacij in zaščito, prilagojeno tveganju.

11.7.2 DSS05.02: obravnava uveljavljanje kontrol na podlagi razvrstitve in spremljanje.