					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P13S					Naziv dokumenta: **Politika klasifikacije i označavanja podataka**							
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 5.3, 8	
ISO/IEC 27002:2022	Kontrole 5.12, 5	
NIST SP 800-53 Rev.5	AC-16, MP-3, MP-5	
EU NIS2	Članak 21(2)(a)	
EU DORA	Članak 5(8)	
COBIT 2019	BAI03.05, DSS05	
EU GDPR	Članak 5, 32	

1. Svrha

1.1 Ova politika definira način na koji se sve informacije kojima organizacija upravlja moraju klasificirati i označavati kako bi se tijekom cijelog njihova životnog ciklusa očuvala njihova povjerljivost, cjelovitost i dostupnost.

1.2 Ova politika omogućuje dosljedno postupanje s podacima dodjeljivanjem odgovarajućih razina zaštite informacijama na temelju njihove osjetljivosti, utjecaja na poslovanje ili zakonskih obveza.

1.3 Klasifikacija i označavanje pomažu smanjiti rizik od slučajnog otkrivanja, neovlaštenog pristupa ili nepravilnog postupanja s osjetljivim podacima, osobito u SME okruženjima koja se mogu oslanjati na jednostavnije sustave i manji broj formaliziranih kontrola.

1.4 Ova politika ključna je za certifikaciju prema normi ISO/IEC 27001 i usklađenost s regulatornim zahtjevima, osobito sa zakonima o zaštiti podataka kao što je GDPR te okvirima kibernetičke sigurnosti kao što su NIS2 i DORA.

2. Opseg

2.1 Ova politika primjenjuje se na sve podatke organizacije, neovisno o formatu ili lokaciji, uključujući:

2.1.1 elektroničke dokumente, proračunske tablice, poruke e-pošte, obrasce, slike i skenirane datoteke

2.1.2 fizičke dokumente kao što su ispisani zapisi, izvješća, računi i bilješke

2.1.3 podatke pohranjene ili obrađene u uslugama u oblaku, na lokalnim poslužiteljima, prijenosnim medijima ili osobnim uređajima koji se koriste u poslovne svrhe

2.1.4 privremene ili prolazne podatke nastale tijekom poslovnih aktivnosti (npr. zapisnike dnevnika, privremene datoteke, poruke e-pošte)

2.2 Svo osoblje, ugovorni izvođači, privremeno osoblje i vanjski pružatelji usluga s pristupom podacima organizacije moraju se pridržavati ove politike.

2.3 Ova politika primjenjuje se tijekom cijelog životnog ciklusa podataka — od izrade i pohrane, preko pristupa i prijenosa, do arhiviranja ili brisanja.

3. Ciljevi

3.1 Definirati jednostavnu i provedivu klasifikacijsku shemu koju je moguće lako razumjeti i primjenjivati u cijeloj organizaciji.

3.2 Zahtijevati da svaki podatkovni resurs bude klasificiran prema svojoj osjetljivosti i odgovarajuće označen radi pravilnog postupanja, pohrane i pristupa.

3.3 Osigurati da su prakse označavanja podataka integrirane u poslovne procese kao što su uvođenje u posao, pokretanje projekata i uspostava sustava.

3.4 Smanjiti rizik od povreda podataka primjenom kontrola postupanja (npr. šifriranje, ograničenje pristupa) u skladu s razinom klasifikacije.

3.5 Osigurati usklađenost sa zakonima o privatnosti i informacijskoj sigurnosti dokazivanjem da su osjetljivi podaci (npr. osobni, financijski ili vlasnički) pravilno označeni i da se njima pravilno upravlja.

3.6 Uspostaviti odgovornost za odluke o klasifikaciji te osigurati periodične preglede i ažuriranja na temelju promjenjivih poslovnih i pravnih potreba.

4. Uloge i odgovornosti

4.1 Glavni direktor (GM)

4.1.1 Vlasnik je ove politike i odobrava klasifikacijsku shemu.

4.1.2 Osigurava nadzor kako bi se odgovornosti za klasifikaciju delegirale i provodile.

4.1.3 Pregledava i odobrava sve iznimke od zahtjeva za klasifikaciju ili označavanje.

4.1.4 Osigurava da prakse postupanja s podacima ispunjavaju zahtjeve usklađenosti prema zakonima kao što su GDPR i DORA.

4.2 Vlasnik informacija / voditelj podataka

4.2.1 Dodjeljuje početnu klasifikaciju svakom novom skupu podataka ili informacijskoj imovini pri izradi ili pribavljanju.

4.2.2 Osigurava da se, gdje je primjenjivo, primjenjuju vidljive oznake (npr. zaglavlja datoteka, podnožja, vodeni žigovi, nazivi mapa).

4.2.3 Periodično pregledava klasifikacije radi provjere relevantnosti, točnosti i svih potrebnih promjena (npr. nakon deklasifikacije ili objave).

4.2.4 Surađuje s voditeljem IT-a radi provedbe tehničkih zaštitnih mjera na temelju klasifikacije (npr. prava pristupa, šifriranje).

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

9. Pregled i ažuriranje zahtjeva

9.1 Ovu politiku moraju jednom godišnje pregledati GM i voditelj podataka kako bi se osiguralo da odražava:

9.1.1 promjene u poslovnim aktivnostima ili vrstama podataka

9.1.2 nove regulatorne zahtjeve (npr. u području privatnosti podataka ili financijskog nadzora)

9.1.3 tehnološke promjene koje utječu na mogućnosti označavanja ili klasifikacije

9.2 Pregled mora uključivati ažuriranja klasifikacijskih kategorija, alata ili praksi označavanja te sadržaja za podizanje svijesti i obuku.

9.3 Izmjene politike mora odobriti GM, a o njima moraju biti obaviješteni svi zaposlenici. Evidencija promjena verzija mora se zadržati za potrebe revizije.

10. Povezane politike i poveznice

10.1 P2S – Politika uloga i odgovornosti u upravljanju: dodjeljuje odgovornost za vlasništvo nad politikom i njezinu provedbu.

10.2 P4S – Politika kontrole pristupa: usklađuje pristup sustavu s razinama klasifikacije podataka.

10.3 P12S – Politika upravljanja imovinom: prati fizičku i digitalnu imovinu u kojoj se pohranjuju klasificirani podaci.

10.4 P17S – Politika zaštite podataka i privatnosti: uređuje zaštitu osobnih podataka, od kojih je velik dio klasificiran kao Povjerljivo.

10.5 P30S – Politika odgovora na incidente: definira putove eskalacije i postupke odgovora u slučaju kršenja klasifikacije ili izlaganja podataka.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 5.3: zahtijeva jasno definirane odgovornosti za postupanje s podacima i njihovu zaštitu.

11.1.2 Točka 8.1: zahtijeva operativno planiranje i kontrole, uključujući one povezane s kategorizacijom podataka.

11.2 ISO/IEC 27002

11.2.1 Kontrola 5.12: daje smjernice za klasifikaciju informacija na temelju rizika i regulatornih zahtjeva.

11.2.2 Kontrola 5.13: opisuje praktične mehanizme označavanja i povezana pravila postupanja.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-16: zahtijeva označavanje informacija kako bi zaštitne mjere bile usklađene s klasifikacijom.

11.3.2 MP-3 / MP-5: daju smjernice za označavanje i kontrolu medija i izlaznih sadržaja.

11.4 EU GDPR

11.4.1 Članci 5 i 32: zahtijevaju minimizaciju podataka i cjelovitost primjenom odgovarajuće klasifikacije i zaštitnih mjera postupanja.

11.5 EU NIS

11.5.1 Članak 21(2)(a): propisuje tehničke i organizacijske kontrole za zaštitu podataka utemeljene na riziku.

11.6 EU DORA

11.6.1 Članak 5(8): zahtijeva da organizacije klasificiraju podatkovnu imovinu kao dio svojeg programa upravljanja IKT rizicima.

11.7 COBIT 2019

11.7.1 BAI03.05: zahtijeva klasifikaciju informacija i zaštitu prilagođenu riziku.

11.7.2 DSS05.02: odnosi se na provedbu kontrola temeljenih na klasifikaciji i njihovo praćenje.