					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P13					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**

1. Svrha

1.1 Ova politika definira formalni okvir za klasifikaciju i označavanje informacijske imovine organizacije na temelju osjetljivosti, izloženosti riziku i regulatornih obveza.

1.2 Njome se osigurava da su sve informacije — bilo pohranjene, prenesene ili obrađene — jasno kategorizirane i označene na način koji komunicira potrebnu razinu zaštite i postupanja.

1.3 Ova politika propisuje strukturiranu klasifikaciju usklađenu s praksama upravljanja rizicima organizacije, uz potporu ciljevima povjerljivosti, cjelovitosti i dostupnosti za digitalne i fizičke oblike podataka.

1.4 Ova kontrola ključna je za omogućavanje pristupa temeljenog na ulogama, spremnosti za reviziju, primjerenog dijeljenja podataka i učinkovite primjene tehničkih zaštitnih mjera kao što su šifriranje, sigurnosne kopije i praćenje.

2. Područje primjene

2.1 Ova politika primjenjuje se na:

2.1.1 svu informacijsku imovinu organizacije, uključujući dokumente, baze podataka, zapise i komunikaciju

2.1.2 sve formate podataka, uključujući digitalne, tiskane, pisane i usmene

2.1.3 sva okruženja: lokalna, udaljena, mobilna i okruženja u oblaku

2.1.4 sve zaposlenike, ugovorne izvođače, pružatelje usluga i izvršitelje obrade trećih strana koji stvaraju, obrađuju ili pohranjuju informacije organizacije

2.2 Područje primjene obuhvaća interno razvijen sadržaj, podatke pribavljene iz vanjskih izvora, osobne podatke koji podliježu obvezama iz propisa o zaštiti privatnosti (npr. GDPR EU) te informacije razmijenjene s klijentima, partnerima i regulatorima.

2.3 Primjenjuje se na sve sustave koji se koriste za pohranu ili prijenos podataka, uključujući poslovne aplikacije, datotečne poslužitelje, sustave elektroničke pošte, platforme u oblaku i repozitorije sigurnosnih kopija.

3. Ciljevi

3.1 Uspostaviti standardiziranu klasifikacijsku shemu na razini cijele organizacije na temelju utjecaja izloženosti ili kompromitacije podataka.

3.2 Osigurati da su sve informacije vidljivo i trajno označene tako da odražavaju svoju razinu klasifikacije i zahtjeve za postupanje.

3.3 Osigurati provedbu kontrola postupanja s podacima i kontrola pristupa usklađenih s klasifikacijom, uključujući šifriranje, zapisivanje dnevnika, zaštitu prijenosa i raspored zadržavanja.

3.4 Podržati usklađenost s međunarodnim standardima (ISO/IEC 27001, 27002), pravnim okvirima (GDPR, NIS2, DORA) i internim politikama upravljanja rizicima.

3.5 Osigurati da svi korisnici razumiju svoje odgovornosti u zaštiti podataka, primjeni oznaka i ispravnom postupanju s klasificiranim informacijama.

3.6 Održavati sljedivost između statusa klasifikacije, povezanih kontrola i Popisa imovine organizacije za potrebe revizije i usklađenosti.

4. Uloge i odgovornosti

4.1 glavni direktor za informacijsku sigurnost (CISO)

4.1.1 Odgovoran je za Politiku klasifikacije i označavanja podataka te osigurava njezinu usklađenost s regulatornim, ugovornim i operativnim zahtjevima.

4.1.2 Odobrava razine klasifikacije, standarde označavanja i izmjene politike.

4.1.3 Nadzire usklađenost s politikom putem revizija, metrika i pregleda iznimaka.

4.1.4 Koordinira međufunkcionalno upravljanje s timovima za pravne poslove, zaštitu privatnosti podataka i upravljanje rizicima.

4.2 Vlasnici informacija

4.2.1 Odgovorni su za klasifikaciju informacijske imovine pod svojom kontrolom primjenom klasifikacijske sheme organizacije.

4.2.2 Primjenjuju klasifikacijske oznake u trenutku nastanka, ažuriranja ili zaprimanja informacija.

4.2.3 Periodično pregledavaju klasifikaciju imovine, osobito kao odgovor na promjene osjetljivosti, regulatornog opsega ili poslovne vrijednosti.

4.2.4 Osiguravaju da se s osjetljivim podacima pravilno postupa i da su primjereno označeni tijekom cijelog životnog ciklusa.

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

9. Zahtjevi za pregled i ažuriranje

9.1 Ova politika mora se pregledati najmanje jednom godišnje kako bi se osigurala usklađenost sa:

9.1.1 razvojem regulatornih zahtjeva (npr. GDPR, NIS2, DORA)

9.1.2 ažuriranjima smjernica ISO/IEC 27001 ili 27002 za klasifikaciju

9.1.3 organizacijskim promjenama koje utječu na osjetljivost podataka ili vlasništvo

9.1.4 tehnološkim promjenama, uključujući nove platforme za upravljanje dokumentima ili podacima

9.2 glavni direktor za informacijsku sigurnost (CISO) pokreće pregled u suradnji s Odborom za informacijsku sigurnost, pravnim savjetnikom i pogođenim poslovnim jedinicama.

9.3 Pregledi moraju uključivati:

9.3.1 djelotvornost provedbe klasifikacije i pridržavanje korisnika

9.3.2 analizu incidenata ili iznimaka povezanih s pogrešnom klasifikacijom

9.3.3 povratne informacije korisnika o alatima za označavanje ili smjernicama

9.3.4 usporedbu sa standardima klasifikacije u industriji

9.4 Ažuriranja politike moraju biti pod verzijskom kontrolom, dokumentirana u repozitoriju dokumenata ISMS-a i priopćena svom relevantnom osoblju s naglaskom na nove odgovornosti ili promjene alata.

9.5 Novi zaposlenici moraju biti upoznati s važećom verzijom politike tijekom uvođenja u posao. Svi zaposlenici moraju završiti obnovnu obuku nakon značajnih promjena politike.

10. Povezane politike i poveznice

10.1 Ovu politiku izravno podupiru i provode kontrole opisane u sljedećim povezanim politikama:

10.1.1 P4 - Politika kontrole pristupa: pristup informacijama uređuje se prema razinama klasifikacije; osjetljiviji podaci zahtijevaju strože mehanizme kontrole pristupa i autorizacije.

10.1.2 P11 - Politika upravljanja korisničkim računima i privilegijama: podupire dodjelu privilegija na temelju načela nužnog poznavanja, koje je određeno klasifikacijskim razinama.

10.1.3 P12 - Politika upravljanja imovinom: osigurava da svaka stavka imovine u Popisu imovine uključuje svoju klasifikaciju i oznaku, čime podupire sljedivost i odgovornost.

10.1.4 P14 - Politika zadržavanja i zbrinjavanja podataka: pravila zadržavanja i zbrinjavanja određuju se prema razini klasifikacije podataka i regulatornim zahtjevima za zadržavanje.

10.1.5 P18 - Politika kriptografskih kontrola: primjenjuje odgovarajuće standarde šifriranja na temelju klasifikacije informacijske imovine.

10.1.6 P22 - Politika bilježenja i praćenja: omogućuje praćenje pristupa klasificiranim informacijama i njihova kretanja te osigurava revizivost i otkrivanje pogrešnog označavanja ili zlouporabe.

10.2 Svaka poveznica osigurava dosljednu zaštitu informacija tijekom njihova životnog ciklusa, od nastanka i klasifikacije do sigurnog postupanja, pohrane, prijenosa i konačnog uništenja.

11. Referentni standardi i okviri

11.1 Ova politika usklađena je s međunarodno priznatim standardima i regulatornim okvirima koji uređuju klasifikaciju i označavanje osjetljivih informacija.

11.2 ISO/IEC 27001

11.2.1 Točka 4.2 - Razumijevanje potreba i očekivanja zainteresiranih strana. Zahtjevi za klasifikaciju često proizlaze iz pravnih, regulatornih ili ugovornih obveza koje nameću zainteresirane strane (npr. GDPR, ugovori o povjerljivosti klijenata), a koje se moraju odraziti u ovoj politici.

11.2.2 Točka 6.1.3 - Obrada rizika informacijske sigurnosti. Klasifikacija izravno utječe na odabir kontrola obrade rizika, uključujući kontrolu pristupa, šifriranje i zadržavanje, na temelju osjetljivosti podataka.

11.2.3 Točka 7.2 - Kompetentnost. Ova politika propisuje da osoblje odgovorno za klasifikaciju i označavanje mora biti osposobljeno, što spada u zahtjeve kompetentnosti.

11.2.4 Točka 7.3 - Svijest. Ova politika zahtijeva da svi korisnici budu upoznati s klasifikacijskim razinama i svojim odgovornostima u postupanju s informacijama, čime se usklađuje s obvezama podizanja svijesti.

11.2.5 Točka 7.5 - Dokumentirane informacije. Sama politika klasifikacije kontrolirani je dokument, a postupci, zapisi o obuci i klasifikacijske oznake dio su dokumentiranih informacija.

11.2.6 Točka 8.1 - Operativno planiranje i kontrola. Klasifikacija i označavanje operativni su procesi ugrađeni u upravljanje životnim ciklusom podataka, a ova točka osigurava da se takve aktivnosti planiraju, provode i kontroliraju.

11.2.7 Točka 9.1 - Praćenje, mjerenje, analiza i vrednovanje. Ova politika uključuje odredbe za praćenje usklađenosti klasifikacije, trendova incidenata i djelotvornosti sheme označavanja.

11.2.8 Točka 10.1 - Nesukladnost i korektivna radnja. Ova politika definira odgovore na pogrešnu klasifikaciju, uključujući korektivne radnje kao što su ponovno osposobljavanje, ažuriranja i postupanje s iznimkama.

11.3 ISO/IEC 27002:2022

11.3.1 Kontrola 5.12 - Klasifikacija informacija. Ova kontrola osigurava da se informacije klasificiraju na temelju svoje osjetljivosti, vrijednosti i kritičnosti — upravo ono što ova politika formalizira.

11.3.2 Kontrola 5.13 - Označavanje informacija. Ova kontrola zahtijeva odgovarajuće označavanje informacija u skladu s njihovom razinom klasifikacije, što je ovom politikom u cijelosti obuhvaćeno.

11.3.3 Kontrola 5.10 - Prihvatljiva uporaba imovine organizacije. Ova politika propisuje kako korisnici trebaju postupati s klasificiranim podacima, čime izravno podupire prihvatljivu uporabu i sprječava zlouporabu.

11.3.4 Kontrola 5.11 - Povrat imovine. Klasifikacija pomaže osigurati da se osjetljivi podaci identificiraju i sigurno vrate ili saniraju kada zaposlenik ili dobavljač odlazi.

11.3.5 Kontrola 5.9 - Popis informacija i druge povezane imovine. Klasifikacija je često povezana s Popisom imovine, koji mora odražavati razinu klasifikacije svake stavke radi pravilne dodjele kontrola.

11.3.6 Kontrola 5.14 - Prijenos informacija. Razine klasifikacije utječu na kontrole unutarnjih i vanjskih prijenosa podataka (npr. šifriranje, odobravanje, ograničenja pristupa).

11.3.7 Kontrola 8.12 - Sprječavanje curenja podataka. Provedba klasifikacije i označavanja podupire sprječavanje neovlaštenog otkrivanja i gubitka podataka.

11.3.8 Kontrola 8.11 - Maskiranje podataka. Određene razine klasifikacije (npr. Povjerljivo, Ograničeno) mogu zahtijevati maskiranje kada se podaci koriste u testnim/razvojnim okruženjima ili analitici.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-2 - Politika i postupci zaštite sustava i komunikacija: podupire politike klasifikacije kao dio sveobuhvatne zaštite podataka.

11.4.2 AC-16 - Sigurnosni atributi: provodi kontrolu pristupa na temelju klasifikacijskih metapodataka i korisničkih ovlaštenja.

11.4.3 MP-3 / MP-5 - Označavanje medija i zaštita tijekom prijenosa: provodi označavanje i zaštitu podataka u mirovanju i tijekom prijenosa na temelju klasifikacije.

11.5 GDPR EU (2016/679)

11.5.1 Članak 5 - Načela zaštite podataka: zahtijeva da se osobni podaci obrađuju sigurno i razmjerno njihovoj osjetljivosti.

11.5.2 Članak 32 - Sigurnost obrade: potvrđuje klasifikaciju kao mehanizam zaštite podataka temeljen na riziku i primjerenim tehničkim mjerama.

11.6 Direktiva EU NIS2 (2022/2555)

11.6.1 Članak 21(2)(a): zahtijeva politike za upravljanje rizicima informacijske sigurnosti, uključujući kontrole klasifikacije imovine i podataka.

11.6.2 Članak 21(3): potiče usvajanje mjera za provedbu primjerenog postupanja s podacima — poduprto označavanjem temeljenim na klasifikaciji.

11.7 Uredba EU DORA (2022/2554)

11.7.1 Članak 5 - Upravljanje i kontrola: zahtijeva okvire upravljanja koji klasificiraju podatkovnu imovinu radi kontrole IKT rizika.

11.7.2 Članak 9 - Upravljanje IKT rizicima: nameće tehničke i organizacijske mjere za kritičnu IKT imovinu, uključujući klasifikaciju i označavanje.

11.8 COBIT 2019

11.8.1 DSS05.02 - Upravljanje sigurnosnim uslugama: provodi klasifikaciju informacijske sigurnosti kako bi se osigurala zaštita podataka organizacije.

11.8.2 MEA03 - Praćenje, vrednovanje i procjena usklađenosti: podupire redovitu reviziju i pregled klasifikacijskih praksi radi osiguravanja pridržavanja politike i zrelosti procesa.