					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P03					Naziv dokumenta: **Politika prihvatljivog korištenja**							
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 regulativom

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 5	Utvrđuje pravila ponašanja i zahtjeve za Politiku prihvatljivog korištenja (AUP)
ISO/IEC 27002:2022	Kontrole 6.1, 6.2, 8.1, 8.12	Usmjerava odgovornosti za informacijsku sigurnost, podizanje svijesti te upravljanje uređajima i podacima
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Kontrola pristupa te kontrole podizanja svijesti i pravila ponašanja relevantne za korištenje IT imovine
GDPR EU	Članci 5(1)(f), 32; uvodna izjava 39	Osigurava povjerljivost i cjelovitost, nalaže tehničke i organizacijske kontrole te pravne osnove za pravilno korištenje
Direktiva EU NIS2	Članak 21(2)(a–d)	Nalaže operativne politike i obuku za sigurno korištenje
Uredba EU DORA	Članak 5	Podupire upravljanje ICT rizicima uređivanjem ponašanja korisnika
COBIT 2019	APO07, BAI05, DSS05, MEA01	Upravljanje ljudskim resursima, promjenama, sigurnosnim uslugama te praćenje usklađenosti i učinkovitosti

1. Svrha

1.1 Ova politika definira prihvatljivo i neprihvatljivo korištenje informacijskih sustava organizacije, računalnih resursa, komunikacijskih alata i praksi postupanja s podacima.

1.2 Njome se osigurava da svi korisnici razumiju svoje odgovornosti pri korištenju korporativne IT imovine te da njihove aktivnosti podupiru povjerljivost, cjelovitost, dostupnost i zakonitu obradu informacija.

1.3 Ova politika ispunjava zahtjev točke 5.10 norme ISO/IEC 27001:2022 uspostavom pravila ponašanja za korištenje sustava te primjenom tehničkih i proceduralnih zaštitnih mjera radi smanjenja rizika od zlouporabe, nemara ili nepropisnog postupanja.

1.4 Ova politika također podupire aktivnosti istrage i provedbe, uključujući odgovor na incidente i stegovne mjere za kršenja.

2. Područje primjene

2.1 Ova se politika primjenjuje na sve osobe i subjekte kojima je odobren pristup informacijskim sustavima i imovini organizacije, uključujući, ali ne ograničavajući se na:

2.1.1 zaposlenike, ugovorne izvođače, konzultante, pripravnike i agencijsko osoblje

2.1.2 dobavljače trećih strana s pristupom sustavima ili delegiranim administrativnim ulogama

2.1.3 goste ili partnere koji koriste IT infrastrukturu u vlasništvu organizacije ili koju je organizacija odobrila

2.2 Područje primjene obuhvaća svu tehnološku i podatkovnu imovinu organizacije, uključujući:

2.2.1 radne stanice, prijenosna računala, mobilne uređaje i poslužitelje

2.2.2 mrežnu infrastrukturu i usluge u oblaku

2.2.3 e-poštu, razmjenu poruka, pohranu datoteka, platforme za suradnju i VPN

2.2.4 podatke u mirovanju, prijenosu ili obradi, neovisno o formatu ili lokaciji

2.2.5 svaki osobni uređaj koji se koristi u okviru aranžmana korištenja vlastitih uređaja (BYOD) i koji se povezuje na sustave organizacije

2.3 Ova se politika provodi u svim radnim okruženjima, uključujući:

2.3.1 korporativne urede i produkcijske lokacije

2.3.2 lokacije za rad na daljinu ili hibridna radna okruženja

2.3.3 terenske operacije ili prostore kojima upravljaju treće strane

2.4 Svi korisnici moraju potvrditi upoznatost s ovom politikom i pridržavati je se kao uvjet za pristup sustavima društva ili rukovanje korporativnim podacima.

3. Ciljevi

3.1 Definirati i osigurati provedbu pravila za prihvatljivo korištenje imovine organizacije u području IT resursa.

3.2 Spriječiti neovlašteni pristup, curenje podataka ili štetu nastalu uslijed nemarnog ili zlonamjernog korištenja.

3.3 Zaštititi mreže, imovinu i podatke društva od prijetnji koje proizlaze iz ponašanja korisnika.

3.4 Poduprijeti zakonske i ugovorne obveze dokazivanjem dužne pažnje u upravljanju IT resursima.

3.5 Osigurati dosljednost i jasnoću u primjeni stegovnih mjera i postupaka upravljanja iznimkama.

3.6 Promicati kulturu etičnog, sigurnog i odgovornog korištenja digitalnih i fizičkih računalnih resursa.

4. Uloge i odgovornosti

4.1 Izvršno rukovodstvo

4.1.1 Odobrava Politiku prihvatljivog korištenja (AUP) i osigurava njezinu usklađenost s poslovnim ciljevima, regulatornim zahtjevima i vrijednostima organizacije.

4.1.2 Dodjeljuje resurse za provedbu, osposobljavanje, nadzor i preispitivanje politike.

4.1.3 U okviru upravljanja ISMS-om preispituje status usklađenosti i stegovne mjere povezane s kršenjima politike.

4.2 IT i timovi informacijske sigurnosti

4.2.1 Provode tehničke zaštitne mjere radi primjene ove politike, uključujući:

4.2.2 filtriranje sadržaja, zaštitu od zlonamjernog softvera, alate za sigurnost krajnjih točaka i alate za nadzor mreže

4.2.3 sigurnosne konfiguracije e-pošte i rješenja za sprječavanje gubitka podataka (DLP)

4.2.4 blok-liste i popise dopuštenih za softver, hardver i internetske stranice

4.2.5 Održavaju popis odobrenog i zabranjenog softvera, uređaja i usluga.

4.2.6 Istražuju sumnje na kršenja AUP-a, prikupljaju forenzičke dokaze te prema potrebi podupiru stegovne ili pravne radnje.

4.2.7 Surađuju s ljudskim resursima i pravnom funkcijom u vezi s postupanjem po incidentima, eskalacijom i obvezama prijavljivanja.

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

9. Zahtjevi za pregled i ažuriranje

9.1 Okidači i učestalost pregleda

9.1.1 Ova politika mora se preispitivati:

9.1.1.1 najmanje jednom godišnje

9.1.1.2 nakon svake značajne promjene tehnologije ili infrastrukture

9.1.1.3 nakon incidenata ili nalaza revizije koji ukazuju na nedostatke u provedbi

9.1.1.4 kao odgovor na promjene primjenjivih propisa ili ugovora

9.2 Vlasništvo i odobravanje

9.2.1 Glavni službenik za informacijsku sigurnost (CISO) ili imenovani voditelj ISMS-a odgovoran je za postupak pregleda.

9.2.2 Ažuriranja mora odobriti izvršno rukovodstvo i o njima se mora obavijestiti cijela organizacija.

9.2.3 Potvrda upoznatosti s ažuriranim odredbama mora se ponovno prikupiti pri ponovnom izdavanju politike.

9.3 Upravljanje dokumentom

9.3.1 Politika mora sadržavati sljedeće metapodatke i podatke o verzioniranju:

9.3.1.1 naslov, identifikator i razinu klasifikacije

9.3.1.2 vlasnika politike i skrbnika dokumenta

9.3.1.3 povijest promjena i obrazloženje ažuriranja

9.3.1.4 datume pregleda i sljedećeg planiranog ažuriranja

9.3.1.5 reference na zapisnik distribucije i potvrdu upoznatosti

9.3.2 Izvorni primjerak mora se čuvati u repozitoriju dokumenata ISMS-a uz upravljanje verzijama.

10. Povezane politike i upućivanja

10.1 Ova politika mora se tumačiti zajedno sa sljedećim dokumentima:

10.1.1 P1 – Politika informacijske sigurnosti: utvrđuje temeljna očekivanja ponašanja i opredijeljenost višeg rukovodstva za prihvatljivo korištenje.

10.1.2 P4 – Politika kontrole pristupa: definira ovlaštenja i prava povezana s korisnicima, sustavima i pristupom podacima te izravno uspostavlja granice prihvatljivog korištenja.

10.1.3 P6 – Politika upravljanja rizicima: obrađuje rizike povezane s ponašanjem i podupire praćenje i obradu prijetnji koje proizlaze iz aktivnosti korisnika.

10.1.4 P7 – Politika uvođenja u posao i prestanka radnog odnosa: osigurava da se uvjeti prihvatljivog korištenja potvrde pri stupanju u organizaciju i opozovu pri odlasku.

10.1.5 P9 – Politika rada na daljinu: proširuje odredbe prihvatljivog korištenja na rad na daljinu i hibridna radna okruženja.

10.2 Ove povezane politike čine slojeviti model obrane za upravljanje ponašajnim, tehničkim i ugovornim aspektima.

11. Referentni standardi i okviri

11.1 Ova Politika prihvatljivog korištenja (AUP) usklađena je s međunarodno priznatim standardima i pravnim okvirima kako bi se osigurale provedive, revizijski dokazive i na riziku utemeljene kontrole ponašanja u svim oblicima korištenja digitalnih i fizičkih informacijskih sustava.

11.2 ISO/IEC 27001:2022

11.2.1 Točka 5.10 – Prihvatljiva uporaba informacija i druge povezane imovine: ova politika izravno ispunjava zahtjev za definiranjem, priopćavanjem i provedbom pravila kojima se uređuje primjereno korištenje IT resursa.

11.2.2 Dodatak A, kontrola 6.1 – Odgovornosti za informacijsku sigurnost: dodjeljuje jasne odgovornosti za ponašanje korisnika i nadzor usklađenosti.

11.2.3 Dodatak A, kontrola 6.2 – Podizanje svijesti, obrazovanje i osposobljavanje o informacijskoj sigurnosti: ugrađeni procesi osposobljavanja i potvrde upoznatosti s politikom dio su provedbe AUP-a.

11.2.4 Dodatak A, kontrola 8.1 – Uređaji krajnjih korisnika i 8.12 – sprječavanje gubitka podataka (DLP): obuhvaća prihvatljivo ponašanje na korisničkim uređajima i uređuje aktivnosti koje mogu dovesti do izlaganja podataka ili njihova curenja.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-19 (kontrola pristupa za mobilne uređaje) i AC-20 (korištenje vanjskih informacijskih sustava): ova politika definira obveze i ograničenja korisnika za BYOD i pristup sustavima trećih strana.

11.3.2 PL-4 (pravila ponašanja): daje detaljne zahtjeve prihvatljivog korištenja usklađene s ovom politikom.

11.3.3 AT-2 (obuka o sigurnosnoj svijesti): poduprto je osposobljavanjem korisnika i dokumentiranom potvrdom upoznatosti s politikom.

11.3.4 AU-2 (revizijski događaji) i AU-12 (generiranje revizijskih zapisa): provedba se oslanja na praćenje aktivnosti korisnika i upozoravanje na kršenja.

11.4 GDPR EU (2016/679):

11.4.1 Članak 5(1)(f): osigurava sigurnost i cjelovitost osobnih podataka; ova politika ublažava rizike uvedene ljudskim ponašanjem i neovlaštenim korištenjem.

11.4.2 Članak 32: nalaže tehničke i organizacijske mjere, poput kontrola ponašanja i ograničenja korištenja, radi zaštite osobnih podataka.

11.4.3 Uvodna izjava 39: naglašava potrebu da samo ovlaštene osobe imaju nužan pristup i zakonito koriste podatke.

11.5 Direktiva EU NIS2 (2022/2555):

11.5.1 Članak 21(2)(a–d): zahtijeva operativne politike i obuku za sigurno korištenje sustava, što ovaj AUP osigurava definiranjem ponašanja, praćenja i postupaka provedbe.

11.6 Uredba EU DORA (2022/2554):

11.6.1 Članak 5: ova politika podupire okvir za upravljanje ICT rizicima definiranjem pravila za interakciju čovjeka i sustava te smanjenjem izloženosti kibernetičkim rizicima temeljenima na ponašanju.

11.7 COBIT 2019:

11.7.1 APO07 – Managed Human Resources: provodi odgovornosti korisnika i podizanje svijesti kroz cijeli radni ciklus zaposlenika.

11.7.2 BAI05 – Managed Organizational Change: ugrađuje upravljanje prihvatljivim korištenjem u procese promjena koje utječu na ponašanje korisnika.

11.7.3 DSS05 – Managed Security Services: podupire praćenje aktivnosti korisnika, upozorenja o ponašanju i automatizirane mehanizme odgovora.

11.7.4 MEA01 – Monitor, Evaluate, and Assess Performance and Conformance: politika definira metrike i mehanizme za provjeru usklađenosti korisnika s očekivanim pravilima ponašanja.