					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P03S					Naziv dokumenta: **Politika prihvatljive uporabe**							
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	Točka 5	Relevantno za ukupni opseg politike i njezinu provedbu
ISO/IEC 27002:2022	5.10, 5.11, 5	Smjernice o zahtjevima i kontrolama prihvatljive uporabe
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Obuhvaća uporabu sustava/uređaja, praćenje i osposobljavanje korisnika
GDPR EU	Članci 5(1)(f), 32	Cjelovitost i povjerljivost podataka te sigurnosne mjere
Direktiva EU NIS2	Članak 21(2)(b)	Propisuje odgovarajuće sigurnosne politike i politiku prihvatljive uporabe
Uredba EU DORA	Članak 9	Politika upravljanja IKT rizicima, kontrole i provedba
COBIT 2019	DSS05, BAI	Sigurnosne usluge i upravljanje znanjem

1. Svrha

1.1. Ova politika definira prihvatljivu, odgovornu i sigurnu uporabu sustava, uređaja, pristupa internetu, e-pošte, usluga u oblaku i osobnih uređaja koji se koriste u poslovne svrhe, a koje osigurava društvo ili su odobreni za poslovnu uporabu.

1.2. Ova politika osigurava da pojedinci razumiju svoje obveze pri korištenju informacijskih resursa organizacije te pri zaštiti cjelovitosti podataka, privatnosti i kontinuiteta poslovanja.

1.3. Ova politika podupire usklađenost s normom ISO/IEC 27001:2022 uspostavom jasnih standarda ponašanja korisnika, usklađenih sa zakonskim, ugovornim i regulatornim zahtjevima.

2. Opseg

2.1. Ova politika primjenjuje se na sve osobe koje pristupaju sustavima ili podacima društva, njima upravljaju ili ih koriste, uključujući:

2.1.1. Zaposlenike i ugovorne izvođače

2.1.2. Privremene radnike i vježbenike

2.1.3. Vanjske pružatelje IT usluga

2.2. Ova politika obuhvaća:

2.2.1. Računala, telefone i tablete u vlasništvu društva

2.2.2. Osobne uređaje odobrene za poslovnu uporabu (BYOD)

2.2.3. Mreže društva, platforme u oblaku i softverske usluge

2.2.4. Pristup internetu, sustave e-pošte, dijeljenu pohranu i poslovne aplikacije

2.3. Ova politika primjenjuje se u svim radnim okruženjima — na lokaciji, na daljinu i u hibridnim okruženjima — te tijekom cijelog radnog vremena.

3. Ciljevi

3.1. Ovom politikom utvrđuje se što se smatra prihvatljivom, a što neprihvatljivom uporabom IT sustava.

3.1.1. Smanjiti sigurnosne rizike koji proizlaze iz zlouporabe, neovlaštenog pristupa ili unošenja zlonamjernog softvera.

3.1.2. Zaštititi poslovne podatke, podatke o klijentima i ugled društva.

3.1.3. Uspostaviti provediva pravila i osigurati odgovornost svih korisnika.

3.1.4. Poduprijeti praćenje i usklađenost radi ranog otkrivanja kršenja i poduzimanja korektivnih radnji.

4. Uloge i odgovornosti

4.1. Glavni direktor

4.1.1. Odobrava ovu politiku i odgovoran je za osiguravanje resursa i ovlasti potrebnih za njezinu provedbu.

4.1.2. Pregledava i odobrava sve iznimke od ove politike.

4.2. Voditelj IT-a ili vanjski pružatelj IT usluga

4.2.1. Održava popise odobrenog softvera i hardvera.

4.2.2. Konfigurira uređaje radi provedbe pravila prihvatljive uporabe (npr. filtriranje sadržaja, revizijsko bilježenje pristupa).

4.2.3. Prati korištenje radi utvrđivanja mogućih kršenja i provodi istrage incidenata.

4.2.4. Osigurava da su osobni uređaji (BYOD), ako se koriste u poslovne svrhe, odobreni i sigurno konfigurirani.

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

9. Zahtjevi za pregled i ažuriranje

9.1. Godišnji pregled

9.1.1. Ovu politiku mora pregledati voditelj IT-a najmanje jednom godišnje, uz konačno odobrenje glavnog direktora, kako bi se osiguralo da ostane usklađena s obrascima korištenja tehnologije, novim rizicima i obvezama usklađenosti.

9.2. Pokretači izvanrednog pregleda

9.2.1. Pregledi se moraju provoditi i kao odgovor na:

9.2.2. Nove sustave ili tehnologije (npr. novu uslugu u oblaku ili platformu krajnjih točaka)

9.2.3. Značajna kršenja politike

9.2.4. Izmijenjene zakone ili ugovorne odredbe koje utječu na korištenje IT-a

9.3. Dokumentiranje promjena

9.3.1. Sva ažuriranja moraju se evidentirati u zapisniku verzija koji uključuje:

9.3.1.1. Broj verzije

9.3.1.2. Datum pregleda

9.3.1.3. Sažetak promjena

9.3.1.4. Tijelo koje odobrava

9.4. Komunikacija politike

9.4.1. Revidirane verzije ove politike moraju se dostaviti svim obuhvaćenim korisnicima. Zaposlenici moraju potvrditi primitak i razumijevanje u sklopu svojih obveza povezanih s osposobljavanjem za sigurnosnu svijest.

10. Povezane politike i poveznice

10.1. Ova se politika primjenjuje zajedno s drugim SME politikama kako bi se osigurao cjelovit obuhvat sigurnosnih odgovornosti:

10.1.1. P4S – Politika kontrole pristupa: definira tehničku i proceduralnu provedbu dopuštene uporabe i ograničenja računa.

10.1.2. P8S – Politika podizanja svijesti i osposobljavanja o informacijskoj sigurnosti: osigurava edukaciju korisnika o granicama prihvatljive uporabe i obvezama prijavljivanja.

10.1.3. P9S – Politika rada na daljinu: uređuje korištenje sustava društva izvan lokacije ili iz kućnog okruženja.

10.1.4. P17S – Politika zaštite podataka i privatnosti: uređuje pravila postupanja s osobnim podacima koja se preklapaju s praćenjem prihvatljive uporabe i BYOD-om.

10.1.5. P30S – Politika odgovora na incidente: uređuje postupke za istragu i odgovor na zlouporabu ili kršenje pravila prihvatljive uporabe.

11. Referentni standardi i okviri

11.1. ISO/IEC 27001

11.1.1. Točka 5.10 – Zahtijeva da organizacije definiraju i provode prihvatljivu uporabu imovine organizacije.

11.2. ISO/IEC 27002

11.2.1. Kontrola 5.10 – Daje smjernice za prihvatljivu uporabu sustava, uključujući dopuštena i zabranjena ponašanja.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-19 – Odnosi se na kontrolu uporabe sustava, uključujući osobne uređaje.

11.3.2. AC-20 – Zahtijeva odobravanje i praćenje vanjskih sustava.

11.3.3. AT-2 – Naglašava osposobljavanje korisnika o praksama prihvatljive uporabe.

11.4. GDPR EU

11.4.1. Članak 5(1)(f) – Zahtijeva cjelovitost i povjerljivost osobnih podataka, što može biti ugroženo zlouporabom od strane korisnika.

11.4.2. Članak 32 – Propisuje provedbu tehničkih i organizacijskih mjera za zaštitu sustava i podataka.

11.5. Direktiva EU NIS2

11.5.1. Članak 21(2)(b) – Zahtijeva odgovarajuće sigurnosne politike, uključujući pravila o prihvatljivoj uporabi, radi ublažavanja kibernetičkih prijetnji.

11.6. Uredba EU DORA

11.6.1. Članak 9 – Zahtijeva politike upravljanja IKT rizicima, koje uključuju kontrole uporabe i mehanizme provedbe.

11.7. COBIT 2019

11.7.1. DSS05 – Upravljanje sigurnosnim uslugama: naglašava kontrolu ponašanja korisnika temeljenu na politici.

11.7.2. BAI08 – Upravljanje znanjem: odnosi se na svijest o odgovornostima iz politike i edukaciju o prihvatljivoj uporabi.