					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P08					Naziv dokumenta: **Politika podizanja svijesti i osposobljavanja o informacijskoj sigurnosti**							
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 7.3, Dodatak A kontrola 6.3	Utvrđuje zahtjeve za podizanje svijesti i osposobljavanje obuhvaćene ovom politikom
ISO/IEC 27002:2022	Kontrola 6	Podržava odgovarajuće osposobljavanje za podizanje svijesti temeljeno na radnim ulogama
NIST SP 800-53 Rev.5	AT-1 do AT-5	Usklađeno s politikom i postupcima, obukom za podizanje svijesti, osposobljavanjem temeljenim na ulogama, zapisima o obuci i kontaktom sa sigurnosnim skupinama
GDPR EU	Članci 32, 39; uvodna izjava 78	Propisuje osposobljavanje osoba koje postupaju s osobnim podacima i opću osviještenost zaposlenika
Direktiva EU NIS2	Članci 21(2)(a, b), 21(3)	Zahtijeva politike osposobljavanja o rizicima i sigurnosti te inicijative za podizanje svijesti
Uredba EU DORA	Članci 5, 8, 13	Zahtijeva svijest o IKT rizicima i osposobljavanje kao dio kontrola otpornosti
COBIT 2019	APO07, DSS05, MEA	Dodatno naglašava podizanje svijesti zaposlenika, edukaciju korisnika i praćenje usklađenosti

1. Svrha

1.1 Ova politika uspostavlja formalni okvir kojim se osigurava da je svo osoblje upoznato sa svojim odgovornostima u području informacijske sigurnosti te da primi osposobljavanje potrebno za zaštitu povjerljivosti, cjelovitosti i dostupnosti informacijske imovine.

1.2 Ova politika podržava ISO/IEC 27001 točku 7.3 i Dodatak A kontrolu 6.3 tako što zahtijeva strukturiran program podizanja svijesti i osposobljavanja temeljen na riziku, prilagođen organizacijskim ulogama i promjenjivim prijetnjama.

1.3 Ova politika doprinosi smanjenju ranjivosti povezanih s ljudskim čimbenikom, promicanju sigurnosno osviještenog ponašanja i kontinuiranom jačanju sigurnih praksi u skladu s regulatornim i ugovornim zahtjevima.

2. Područje primjene

2.1 Ova politika primjenjuje se na sve interne i vanjske osobe koje imaju pristup informacijskim sustavima, podacima ili objektima organizacije, uključujući:

2.1.1 zaposlenike (u punom radnom vremenu, nepunom radnom vremenu, privremene)

2.1.2 ugovorne izvođače, konzultante, dobavljače i vježbenike

2.1.3 treće strane s logičkim ili fizičkim pristupom na temelju ugovora o razini usluge

2.2 Opseg obuhvaća:

2.2.1 inicijalnu obuku o sigurnosnoj svijesti pri zapošljavanju

2.2.2 osposobljavanje specifično za ulogu (npr. razvojni inženjeri, financije, korisnici s povlaštenim pristupom)

2.2.3 periodičnu obnovnu obuku i kampanje podizanja svijesti

2.2.4 ad hoc osposobljavanje kao odgovor na incidente ili nove prijetnje

2.3 Metode provedbe osposobljavanja obuhvaćene ovom politikom uključuju e-učenje, radionice uživo, simulacije, provjere znanja, plakate, biltene informacijske sigurnosti i obvezne potvrde upoznatosti.

3. Ciljevi

3.1 Osigurati da svo osoblje razumije svoje odgovornosti u zaštiti imovine organizacije i poštivanju sigurnosnih politika.

3.2 Osigurati kontinuiranu i mjerljivu obuku za podizanje svijesti usklađenu s izloženošću riziku na temelju uloga.

3.3 Ugraditi sigurna ponašanja u svakodnevne operacije jačanjem praksi kao što su sigurna uporaba lozinki, prijavljivanje incidenata i otpornost na phishing.

3.4 Osigurati usklađenost s regulatornim zahtjevima i mogućnost dokazivanja usklađenosti s obveznim zahtjevima za edukaciju o informacijskoj sigurnosti u različitim industrijama i jurisdikcijama.

3.5 Smanjiti sigurnosne incidente koji nastaju zbog nemara, neupućenosti ili loše prosudbe kroz oblikovanje ponašanja i kontinuirano jačanje svijesti.

4. Uloge i odgovornosti

4.1 Izvršno vodstvo

4.1.1 Odobrava strategiju edukacije o informacijskoj sigurnosti organizacije te osigurava potrebne resurse i njezino uključivanje u prioritete organizacije.

4.1.2 Na upravljačkoj razini prati usklađenost i osigurava pridržavanje politike u svim odjelima.

4.2 CISO / voditelj ISMS-a

4.2.1 Vlasnik je ove politike i definira okvir za podizanje svijesti i obuku u skladu s rizicima, zahtjevima usklađenosti i poslovnim potrebama.

4.2.2 Nadzire izradu, provedbu, praćenje i preispitivanje svih inicijativa za sigurnosno osposobljavanje.

4.2.3 Osigurava da se obuka periodično obnavlja i da odražava promjenjive prijetnje i nove tehnologije.

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

9. Zahtjevi za pregled i ažuriranje

9.1 Učestalost pregleda

9.1.1 Ova politika i povezani program osposobljavanja moraju se pregledavati:

9.1.1.1 godišnje, ili

9.1.1.2 nakon većih incidenata koji uključuju ljudsku pogrešku ili insajdersku prijetnju

9.1.1.3 pri uvođenju značajnih novih tehnologija ili prijetnji

9.1.1.4 kao odgovor na promjene pravnih, ugovornih ili certifikacijskih obveza

9.2 Postupak pregleda

9.2.1 Pregled vodi CISO u koordinaciji sa:

9.2.1.1 odjelima ljudskih resursa i osposobljavanja

9.2.1.2 pravnom službom i službenikom za zaštitu podataka

9.2.1.3 funkcijama IT sigurnosti i operativnog rizika

9.2.2 Sve izmjene moraju biti:

9.2.2.1 odobrene od strane Upravljačkog odbora ISMS-a

9.2.2.2 pod verzijskom kontrolom i dokumentirane u registru dokumenata ISMS-a

9.2.2.3 priopćene korisnicima ako bitne izmjene utječu na opseg obuke ili odgovornosti

9.3 Upravljanje ažuriranjem sadržaja

9.3.1 Moduli obuke i materijali za podizanje svijesti moraju se pregledavati svakih 12 mjeseci kako bi se osigurala:

9.3.1.1 relevantnost za okruženje prijetnji

9.3.1.2 regulatorna točnost

9.3.1.3 kompatibilnost formata (npr. pristupačnost, lokalizacija)

9.3.2 Zastarjeli ili obmanjujući sadržaj mora se odmah povući i zamijeniti odobrenim alternativama.

10. Povezane politike i poveznice

10.1 Ovu politiku podržavaju i ona podržava provedbu sljedećih dokumenata:

10.1.1 P01 – Politika informacijske sigurnosti: Uspostavlja podizanje sigurnosne svijesti kao temeljnu kontrolu u sustavu upravljanja informacijskom sigurnošću (ISMS) organizacije.

10.1.2 P03 – Politika prihvatljive uporabe: Zahtijeva potvrdu korisnika tijekom obuke i pojašnjava odgovornosti povezane sa svakodnevnim korištenjem tehnologije.

10.1.3 P07 – Politika uvođenja u posao i prestanka radnog odnosa: Osigurava da je obuka ugrađena pri ulasku u organizaciju i da se prati tijekom cijelog zaposlenja.

10.1.4 P06 – Politika upravljanja rizicima: Povezuje osposobljavanje usmjereno na ljudski čimbenik s modeliranjem prijetnji i strategijama smanjenja preostalog rizika.

10.1.5 P33 – Politika praćenja revizije i usklađenosti: Potvrđuje da su kontrole podizanja svijesti operativne, mjerljive i djelotvorne tijekom revizija.

10.2 Zajedno, ove politike čine sveobuhvatan okvir bihevioralnih kontrola koji objedinjuje podizanje svijesti, odgovornost i jačanje sigurnosne kulture.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 7.3 – Podizanje svijesti: Zahtijeva da organizacije osiguraju da su radnici upoznati s politikama informacijske sigurnosti i svojim odgovornostima. Ova politika provodi taj zahtjev kroz strukturirano uvođenje u posao, periodičnu obuku i mjerljivo sudjelovanje u kampanjama.

11.1.2 Dodatak A kontrola 6.3 – Podizanje svijesti, edukacija i osposobljavanje o informacijskoj sigurnosti: U potpunosti je obuhvaćena kroz inicijalne, ulogama prilagođene i kontinuirane programe obuke prilagođene profilima rizika korisnika.

11.2 ISO/IEC 27002:2022 – Kontrola 6

11.2.1 Podržava razvoj i provedbu obuke za podizanje svijesti primjerene radnim ulogama, s naglaskom na jačanje sigurnog ponašanja i periodična ažuriranja na temelju obavještajnih podataka o prijetnjama i povratnih informacija iz revizije.

11.3 NIST SP 800-53 Rev.5

11.3.1 AT-1 do AT-5 (skupina kontrola Awareness and Training): Ova politika usklađena je s AT-1 (Politika i postupci), AT-2 (Obuka za podizanje svijesti), AT-3 (Osposobljavanje temeljeno na ulogama), AT-4 (Zapisi o sigurnosnoj obuci) i AT-5 (Kontakt sa sigurnosnim skupinama).

11.3.2 IA-5, AC-2: Jača odgovornost korisnika za sigurnu autentifikaciju i prihvatljivu uporabu, što je ključno za bihevioralne ishode programa podizanja svijesti.

11.3.3 IR-1 do IR-8: Spremnost za odgovor na incidente jača se putem ciljanih kampanja podizanja svijesti i simulacija.

11.4 GDPR EU (2016/679)

11.4.1 Članak 32 – Sigurnost obrade: Zahtijeva da osoblje koje postupa s osobnim podacima bude osposobljeno za prepoznavanje, sprječavanje i prijavljivanje rizika za osobne podatke. Ova politika osigurava da su osobe koje postupaju s podacima i sve relevantne uloge odgovarajuće osposobljene.

11.4.2 Članak 39 – Zadaće službenika za zaštitu podataka: Uključuje podizanje svijesti i osposobljavanje osoblja uključenog u postupke obrade.

11.4.3 Uvodna izjava 78: Potiče odgovarajuće mjere podizanja svijesti radi osiguravanja robusnih sigurnosnih praksi i pridržavanja politike.

11.5 Direktiva NIS2 EU (2022/2555)

11.5.1 Članak 21(2)(a, b): Zahtijeva da subjekti usvoje politike o analizi rizika i sigurnosnom osposobljavanju za svo relevantno osoblje. Ova politika ispunjava taj zahtjev uspostavom kontinuiranih procesa obuke prilagođenih ulogama.

11.5.2 Članak 21(3): Potiče promicanje svijesti o kibernetičkim rizicima među upravom i osobljem putem inicijativa podizanja svijesti i simulacija.

11.6 Uredba DORA EU (2022/2554)

11.6.1 Članak 13 – Strategija digitalne operativne otpornosti: Zahtijeva da svijest o IKT rizicima i osposobljavanje budu dio modela upravljanja. Ova politika osigurava da se ljudski rizik adresira kontinuiranom edukacijom i simulacijama prijetnji.

11.6.2 Članci 5 i 8: Naglašavaju važnost okvira internih kontrola, pri čemu su podizanje svijesti i osposobljavanje temeljne sastavnice IKT otpornosti i kibernetičke higijene.

11.7 COBIT 2019

11.7.1 APO07 – Managed Human Resources: Dodatno naglašava potrebu za razvojem svijesti o sigurnosnim odgovornostima i njezinim uključivanjem u upravljanje radnom snagom.

11.7.2 DSS05 – Managed Security Services: Uspostavlja kontrole nad edukacijom korisnika i prijavljivanjem incidenata, što je sastavni dio ove politike.

11.7.3 MEA03 – Monitor, Evaluate, and Assess Compliance: Zahtijeva pregled učinkovitosti ponašanja korisnika i pridržavanja politike, što se ovdje provodi putem phishing testova, kvizova i metrika kampanja podizanja svijesti.