					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P08S					Naziv dokumenta: **Politika podizanja svijesti i osposobljavanja za informacijsku sigurnost**							
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 s primjenjivim standardima i propisima

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Clause 7	
ISO/IEC 27002:2022	Control 6	
NIST SP 800-53 Rev.5	AT-2, AT-4	
EU NIS2	Article 21(2)(i)	
EU DORA	Article 13	
COBIT 2019	BAI08, DSS05	
EU GDPR	Article 32, 39	

1. Svrha

1.1. Ova politika osigurava da svi zaposlenici i ugovorni suradnici razumiju svoje odgovornosti u području informacijske sigurnosti.

1.2. Cilj politike je smanjiti vjerojatnost ljudske pogreške, unaprijediti sposobnost otkrivanja i prijavljivanja incidenata te razvijati kulturu sigurnosne osviještenosti u cijeloj organizaciji.

1.3. Ova politika podupire usklađenost s normom ISO/IEC 27001, direktivom NIS2, GDPR-om i uredbom DORA tako što podizanje svijesti o sigurnosti integrira u svakodnevno radno ponašanje i očekivanja povezana s radnom ulogom.

2. Područje primjene

2.1. Ova politika primjenjuje se na sve zaposlenike, ugovorne suradnike, vježbenike i treće strane koje imaju pristup sustavima ili podacima društva.

2.2. Obuhvaća:

2.2.1. početno osposobljavanje za sigurnosnu svijest pri zapošljavanju novog osoblja

2.2.2. godišnje obnovno osposobljavanje iz područja sigurnosti

2.2.3. ad hoc aktivnosti podizanja svijesti (npr. obavijesti povezane s incidentima, plakati ili sigurnosni savjeti)

2.3. Primjenjuje se na sve radne uloge, organizacijske jedinice i lokacije rada.

3. Ciljevi

3.1. Osigurati da svo osoblje pravodobno primi razumljivo i relevantno osposobljavanje za podizanje svijesti o sigurnosti.

3.2. Omogućiti zaposlenicima da prepoznaju i izbjegnu uobičajene prijetnje kao što su phishing, zlonamjerni softver i curenje podataka.

3.3. Uspostaviti evidenciju o završenom osposobljavanju radi dokazivanja usklađenosti sa zakonskim, ugovornim i revizijskim zahtjevima.

3.4. Održavati ažuran sadržaj osposobljavanja koji odražava politike organizacije, prijetnje i primjenjive propise.

3.5. Poticati proaktivan pristup među osobljem, pri čemu se sigurnost smatra dijelom svakodnevne odgovornosti.

4. Uloge i odgovornosti

4.1. direktor

4.1.1. Odobrava zahtjeve za osposobljavanje i osigurava dodjelu potrebnih resursa.

4.1.2. Pregledava izvješća o završenom osposobljavanju i prema potrebi eskalira slučajeve neusklađenosti.

4.2. voditelj ureda / ljudski resursi (HR)

4.2.1. Koordinira provedbu osposobljavanja za novozaposlene i godišnjeg obnovnog osposobljavanja.

4.2.2. Održava evidenciju osposobljavanja i zapise o dovršetku.

4.2.3. Osigurava da osoblje potvrdi upoznatost s temeljnim politikama informacijske sigurnosti i ugovorima o povjerljivosti.

[... 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 moraju jednom godišnje pregledati direktor i ljudski resursi (HR) kako bi se osiguralo da odražava aktualne rizike, propise i potrebe radne snage.

9.2. Izvanredna ažuriranja

9.2.1. Politika i sadržaj osposobljavanja moraju se također pregledati i revidirati nakon:

9.2.1.1. značajnog sigurnosnog incidenta

9.2.1.2. zakonskih ili ugovornih promjena

9.2.1.3. organizacijskog restrukturiranja ili migracije sustava

9.3. Upravljanje verzijama i distribucija

9.3.1. Svako ažuriranje mora uključivati:

9.3.1.1. broj verzije i datum stupanja na snagu

9.3.1.2. sažetak promjena

9.3.1.3. odobrenje direktora

9.3.1.4. arhivu svih prethodnih verzija, koja se mora čuvati najmanje tri godine

9.4. Komunikacija zaposlenicima

9.4.1. Ažuriranja politike moraju se priopćiti cjelokupnom osoblju, a potvrda upoznatosti mora se pribaviti ako su unesene bitne promjene.

10. Povezane politike i poveznice

10.1. Ova politika podupire sljedeće:

10.1.1. P2S – Politika uloga i odgovornosti u upravljanju: dodjeljuje odgovornost za koordinaciju osposobljavanja i nadzor

10.1.2. P3S – Politika prihvatljive uporabe: dodatno naglašava očekivanja u pogledu ponašanja obrađena u osposobljavanju

10.1.3. P4S – Politika kontrole pristupa: osigurava da korisnici razumiju važnost sigurnosti pristupa

10.1.4. P7S – Politika uvođenja u posao i prestanka radnog odnosa: uključuje osposobljavanje u proces uvođenja u posao

10.1.5. P30S – Politika odgovora na incidente: osigurava da osoblje zna kako pravodobno i ispravno prijaviti incidente

11. Referentni standardi i okviri

11.1. ISO/IEC 27001

11.1.1. Točka 7.3 – Zahtijeva da organizacije osiguraju da je osoblje svjesno svojih odgovornosti i učinaka na sigurnost

11.2. ISO/IEC 27002

11.2.1. Kontrola 6.3 – Detaljno propisuje očekivanja za opseg i provedbu sigurnosnog osposobljavanja

11.3. NIST SP 800-53 Rev.5

11.3.1. AT-2 – Zahtijeva osposobljavanje za podizanje svijesti korisnika koji imaju pristup sustavu

11.3.2. AT-4 – Obuhvaća osposobljavanje temeljeno na ulogama i posljedice neusklađenosti

11.4. GDPR EU

11.4.1. Članak 32 – Propisuje sigurnosne mjere, uključujući osposobljavanje osoblja radi zaštite osobnih podataka

11.4.2. Članak 39 – Zahtijeva da službenici za zaštitu podataka, gdje je primjenjivo, nadziru podizanje svijesti i osposobljavanje

11.5. Direktiva EU NIS2

11.5.1. Članak 21(2)(i) – Zahtijeva kontinuirane programe podizanja svijesti i osposobljavanja u području kibernetičke sigurnosti

11.6. Uredba EU DORA

11.6.1. Članak 13 – Zahtijeva da financijski subjekti provedu edukaciju i osposobljavanje za sve članove osoblja s odgovornostima povezanima s IKT-om

11.7. COBIT 2019

11.7.1. BAI08 – Upravljanje znanjem: osigurava da je osoblje kompetentno i osposobljeno

11.7.2. DSS05 – Upravljanje sigurnosnim uslugama: naglašava podizanje svijesti kao ključnu sigurnosnu kontrolu