					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P08					Naslov dokumenta: **Politika ozaveščanja in usposabljanja na področju informacijske varnosti**							
Različica: 1.0		Datum začetka veljavnosti: 01.01.2025			Lastnik dokumenta:							
X	Politika		Standard		Postopek		Obrazec		Register		Drugo	

Zgodovina revizij				
Številka revizije	**Datum revizije**	**Spremembe**	**Pregledal**	**Lastnik procesa**

Odobritve			
Ime	**Delovno mesto**	**Datum**	**Podpis**

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
ISO/IEC 27001:2022	Klavzula 7.3, Priloga A, kontrola 6.3	Določa zahteve glede ozaveščanja in usposabljanja, ki jih obravnava ta politika
ISO/IEC 27002:2022	Kontrola 6	Podpira ustrezno usposabljanje za ozaveščanje glede na delovno vlogo
NIST SP 800-53 Rev.5	AT-1 do AT-5	Usklajeno s politiko in postopki, usposabljanjem za ozaveščanje, usposabljanjem glede na vloge, evidencami o usposabljanju in stikom z varnostno skupino
Uredba EU GDPR	Člena 32, 39; uvodna izjava 78	Zahteva usposabljanje za obdelovalce osebnih podatkov in splošno ozaveščenost zaposlenih
Direktiva EU NIS2	Člena 21(2)(a, b), 21(3)	Zahteva politike usposabljanja o tveganjih in varnosti ter pobude za ozaveščanje
Uredba EU DORA	Členi 5, 8, 13	Zahteva ozaveščenost o tveganjih IKT in usposabljanje kot del kontrol operativne odpornosti
COBIT 2019	APO07, DSS05, MEA	Krepi ozaveščenost zaposlenih, izobraževanje uporabnikov in spremljanje skladnosti

1. Namen

1.1 Ta politika določa formalni okvir za zagotavljanje, da je vse osebje seznanjeno s svojimi odgovornostmi na področju informacijske varnosti in prejme usposabljanje, potrebno za varovanje zaupnosti, celovitosti in razpoložljivosti (CIA) informacijskih sredstev.

1.2 Podpira ISO/IEC 27001, klavzulo 7.3, in Prilogo A, kontrolo 6.3, tako da zahteva strukturiran program ozaveščanja in na tveganjih temelječega usposabljanja, prilagojen organizacijskim vlogam in spreminjajočim se grožnjam.

1.3 Politika prispeva k zmanjševanju ranljivosti, povezanih s človeškim dejavnikom, spodbuja varnostno ozaveščeno ravnanje in stalno utrjuje varne prakse v skladu z regulatornimi in pogodbenimi zahtevami.

2. Področje uporabe

2.1 Ta politika velja za vse notranje in zunanje posameznike z dostopom do informacijskih sistemov, podatkov ali prostorov organizacije, vključno z:

2.1.1 zaposlenimi (s polnim delovnim časom, s krajšim delovnim časom, začasnimi delavci)

2.1.2 pogodbenimi izvajalci, svetovalci, dobavitelji tretjih oseb in praktikanti

2.1.3 tretjimi osebami z logičnim ali fizičnim dostopom na podlagi storitvenih dogovorov

2.2 Področje uporabe vključuje:

2.2.1 uvodno usposabljanje za varnostno ozaveščanje

2.2.2 usposabljanje, prilagojeno vlogam (npr. razvijalci, finance, uporabniki z visokimi privilegiji)

2.2.3 periodično osvežitveno usposabljanje in kampanje ozaveščanja

2.2.4 ad hoc usposabljanje kot odziv na incidente ali nove grožnje

2.3 Načini izvajanja usposabljanja, zajeti s to politiko, vključujejo e-učenje, osebne seznanitve, simulacije, preverjanje znanja, plakate, varnostne biltene in obvezne potrditve.

3. Cilji

3.1 Zagotoviti, da vse osebje razume svoje odgovornosti pri varovanju sredstev organizacije in upoštevanju varnostnih politik.

3.2 Zagotoviti stalno in merljivo usposabljanje za ozaveščanje, usklajeno z izpostavljenostjo tveganjem glede na vloge.

3.3 Vključiti varno ravnanje v dnevne operativne aktivnosti z utrjevanjem praks, kot so varna uporaba gesel, poročanje o incidentih in odpornost proti lažnemu predstavljanju.

3.4 Zagotoviti skladnost s predpisi in pripravljenost na revizijo glede zahtev usposabljanja za informacijsko varnost v različnih panogah in jurisdikcijah.

3.5 Zmanjšati varnostne incidente, ki izhajajo iz malomarnosti, neozaveščenosti ali slabe presoje, z usmerjanjem vedenja in stalnim utrjevanjem.

4. Vloge in odgovornosti

4.1 Najvišje vodstvo

4.1.1 Odobri strategijo organizacije za usposabljanje na področju informacijske varnosti ter zagotovi potrebne vire in njeno vključitev med korporativne prednostne naloge.

4.1.2 Spremlja skladnost na ravni vodstva in zagotavlja upoštevanje politike v vseh oddelkih.

4.2 Vodja informacijske varnosti / vodja ISMS

4.2.1 Je lastnik te politike in določa okvir ozaveščanja in usposabljanja v skladu s tveganji, zahtevami skladnosti in poslovnimi potrebami.

4.2.2 Nadzira zasnovo, izvedbo, spremljanje in pregled vseh pobud za varnostno usposabljanje.

4.2.3 Zagotavlja, da se usposabljanje periodično posodablja ter odraža spreminjajoče se grožnje in nastajajoče tehnologije.

[... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ...]

9. Zahteve za pregled in posodobitev

9.1 Pogostost pregledov

9.1.1 Ta politika in pripadajoči program usposabljanja se morata pregledati:

9.1.1.1 letno ali

9.1.1.2 po večjih incidentih, povezanih s človeško napako ali notranjo grožnjo

9.1.1.3 ob uvedbi pomembnih novih tehnologij ali groženj

9.1.1.4 kot odziv na spremembe pravnih, pogodbenih ali certifikacijskih obveznosti

9.2 Postopek pregleda

9.2.1 Pregled vodi vodja informacijske varnosti v sodelovanju z:

9.2.1.1 kadrovsko službo in oddelki za usposabljanje

9.2.1.2 pravno službo in pooblaščenimi osebami za varstvo podatkov

9.2.1.3 funkcijami informacijske varnosti in operativnega tveganja

9.2.2 Vse posodobitve morajo biti:

9.2.2.1 odobrene s strani usmerjevalnega odbora ISMS

9.2.2.2 upravljane z različicami in dokumentirane v registru dokumentov ISMS

9.2.2.3 sporočene uporabnikom, če bistvene spremembe vplivajo na področje usposabljanja ali odgovornosti

9.3 Upravljanje posodabljanja vsebine

9.3.1 Module usposabljanja in gradiva za ozaveščanje je treba pregledati vsakih 12 mesecev, da se zagotovi:

9.3.1.1 ustreznost glede na okolje groženj

9.3.1.2 regulatorna skladnost

9.3.1.3 združljivost oblik zapisa (npr. dostopnost, lokalizacija)

9.3.2 Zastarela ali zavajajoča vsebina se mora nemudoma umakniti in nadomestiti z odobrenimi alternativami.

10. Povezane politike in povezave

10.1 To politiko podpirajo in njeno izvajanje dopolnjujejo:

10.1.1 P01 – Politika informacijske varnosti: določa varnostno ozaveščanje kot temeljno kontrolo v sistemu upravljanja informacijske varnosti (ISMS) organizacije.

10.1.2 P03 – Politika sprejemljive uporabe (AUP): zahteva potrditev uporabnika med usposabljanjem in pojasnjuje odgovornosti, povezane z vsakodnevno uporabo tehnologije.

10.1.3 P07 – Politika uvajanja in prenehanja: zagotavlja, da je usposabljanje vključeno ob nastopu dela in spremljano skozi celotno obdobje zaposlitve.

10.1.4 P06 – Politika obvladovanja tveganj: povezuje usposabljanje, osredotočeno na človeški dejavnik, z modeliranjem groženj in strategijami zmanjševanja preostalega tveganja.

10.1.5 P33 – Politika spremljanja presoj in skladnosti: potrjuje, da so kontrole ozaveščanja med presojami operativne, merljive in učinkovite.

10.2 Te politike skupaj tvorijo celovit okvir vedenjskih kontrol, ki združuje ozaveščanje, odgovornost in utrjevanje varnostne kulture.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 7.3 – Ozaveščenost: zahteva, da organizacije zagotovijo, da so delavci seznanjeni s politikami informacijske varnosti in svojimi odgovornostmi. Ta politika to zahtevo uresničuje s strukturiranim uvajanjem, periodičnim usposabljanjem in merljivim sodelovanjem v kampanjah.

11.1.2 Priloga A, kontrola 6.3 – Ozaveščanje, izobraževanje in usposabljanje na področju informacijske varnosti: v celoti je naslovljena z začetnimi programi, programi glede na vloge in stalnimi programi usposabljanja, prilagojenimi profilom tveganja uporabnikov.

11.2 ISO/IEC 27002:2022 – Kontrola 6

11.2.1 Podpira razvoj in izvedbo usposabljanja za ozaveščanje, primernega glede na delovne vloge, s poudarkom na utrjevanju varnega ravnanja in periodičnih posodobitvah na podlagi obveščevalnih podatkov o grožnjah in povratnih informacij iz revizij.

11.3 NIST SP 800-53 Rev.5

11.3.1 AT-1 do AT-5 (družina Ozaveščanje in usposabljanje): ta politika je usklajena z AT-1 (politika in postopki), AT-2 (usposabljanje za ozaveščanje), AT-3 (usposabljanje glede na vloge), AT-4 (evidence o varnostnem usposabljanju) in AT-5 (stik z varnostnimi skupinami).

11.3.2 IA-5, AC-2: krepi odgovornost uporabnikov za varno avtentikacijo in sprejemljivo uporabo, kar je ključno za vedenjske učinke programov ozaveščanja.

11.3.3 IR-1 do IR-8: pripravljenost za odziv na incidente se krepi s ciljno usmerjenimi kampanjami ozaveščanja in simulacijami.

11.4 Uredba EU GDPR (2016/679)

11.4.1 Člen 32 – Varnost obdelave: zahteva, da je osebje, ki obdeluje osebne podatke, usposobljeno za prepoznavanje, preprečevanje in poročanje o tveganjih za osebne podatke. Ta politika zagotavlja, da so obdelovalci osebnih podatkov in vse relevantne vloge ustrezno usposobljeni.

11.4.2 Člen 39 – Naloge pooblaščene osebe za varstvo podatkov: vključuje ozaveščanje in usposabljanje osebja, vključenega v dejavnosti obdelave.

11.4.3 Uvodna izjava 78: spodbuja ustrezne ukrepe ozaveščanja za zagotavljanje robustnih varnostnih praks in upoštevanje politike.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Člen 21(2)(a, b): zahteva, da subjekti sprejmejo politike analize tveganj in varnostnega usposabljanja za vse relevantno osebje. Ta politika to zahtevo izpolnjuje z določitvijo stalnih procesov usposabljanja, prilagojenih vlogam.

11.5.2 Člen 21(3): spodbuja krepitev ozaveščenosti o tveganjih kibernetske varnosti med vodstvom in zaposlenimi prek pobud za ozaveščanje in simulacij.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Člen 13 – Strategija digitalne operativne odpornosti: zahteva, da sta ozaveščenost o tveganjih IKT in usposabljanje del modela upravljanja. Ta politika zagotavlja, da se tveganja, povezana s človeškim dejavnikom, obravnavajo z neprekinjenim izobraževanjem in simulacijami groženj.

11.6.2 Člena 5 in 8: poudarjata pomen okvirov notranjih kontrol, katerih temeljne sestavine za operativno odpornost IKT in kibernetsko higieno sta tudi ozaveščanje in usposabljanje.

11.7 COBIT 2019

11.7.1 APO07 – Upravljani človeški viri: krepi potrebo po razvijanju ozaveščenosti o odgovornostih na področju varnosti in njenem vključevanju v upravljanje delovne sile.

11.7.2 DSS05 – Upravljane varnostne storitve: vzpostavlja kontrole nad izobraževanjem uporabnikov in poročanjem o incidentih, kar je bistveni del te politike.

11.7.3 MEA03 – Spremljanje, vrednotenje in ocenjevanje skladnosti: zahteva pregled učinkovitosti vedenja uporabnikov in upoštevanja politike, kar se tukaj izvaja s testi spletnega ribarjenja, kvizi in kazalniki kampanj ozaveščanja.