					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P08S					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	
ISO/IEC 27002:2022	Kontrola 6	
NIST SP 800-53 Rev. 5	AT-2, AT-4	
EU NIS2	Člen 21(2)(i)	
EU DORA	Člen 13	
COBIT 2019	BAI08, DSS	
EU GDPR	Člen 32, 39	

1. Namen

1.1. Ta politika zagotavlja, da vsi zaposleni in pogodbeni izvajalci razumejo svoje odgovornosti na področju informacijske varnosti.

1.2. Njen namen je zmanjšati verjetnost človeških napak, izboljšati sposobnost zaznavanja in poročanja o incidentih ter krepiti kulturo varnostne ozaveščenosti v celotni organizaciji.

1.3. Politika podpira skladnost z ISO/IEC 27001, NIS2, GDPR in DORA tako, da varnostno ozaveščenost vključuje v vsakodnevne delovne prakse in pričakovanja, vezana na posamezne vloge.

2. Področje uporabe

2.1. Ta politika velja za vse zaposlene, pogodbene izvajalce, praktikante in tretje osebe, ki imajo dostop do sistemov ali podatkov podjetja.

2.2. Vključuje:

2.2.1. uvodno usposabljanje s področja varnostne ozaveščenosti za novo osebje,

2.2.2. redno letno obnovitveno usposabljanje,

2.2.3. ad hoc dejavnosti ozaveščanja (npr. obvestila, povezana z incidenti, plakati ali kratki nasveti).

2.3. Velja za vse delovne vloge, oddelke in lokacije dela.

3. Cilji

3.1. Zagotoviti, da vse osebje pravočasno prejme razumljivo in ustrezno usposabljanje s področja varnostne ozaveščenosti.

3.2. Zaposlenim zagotoviti sposobnost prepoznavanja in izogibanja pogostim grožnjam, kot so napadi z lažnim predstavljanjem, zlonamerna programska oprema in razkritje podatkov.

3.3. Vzpostaviti dokumentiranje opravljenih usposabljanj za dokazovanje skladnosti s pravnimi, pogodbenimi in revizijskimi zahtevami.

3.4. Zagotavljati posodobljene vsebine usposabljanja, ki odražajo politike organizacije, grožnje in veljavne predpise.

3.5. Spodbujati proaktivno naravnanost zaposlenih, pri kateri se varnost obravnava kot del vsakodnevne odgovornosti.

4. Vloge in odgovornosti

4.1. Generalni direktor

4.1.1. Odobri zahteve glede usposabljanja in zagotovi dodelitev ustreznih virov.

4.1.2. Pregleduje poročila o opravljenih usposabljanjih in po potrebi eskalira primere neskladnosti.

4.2. Vodja pisarne / kadrovska služba (HR)

4.2.1. Usklajuje izvedbo usposabljanja za novozaposlene in letnih obnovitvenih usposabljanj.

4.2.2. Vzdržuje evidence in dnevnike usposabljanj.

4.2.3. Zagotavlja pridobitev potrditev zaposlenih glede ključnih politik informacijske varnosti in pogodb o nerazkrivanju informacij.

[... 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. Letni pregled

9.1.1. To politiko morata generalni direktor in kadrovska služba (HR) pregledati najmanj enkrat letno, da se zagotovi njena usklajenost s trenutnimi tveganji, predpisi in potrebami zaposlenih.

9.2. Vmesne posodobitve

9.2.1. Politiko in vsebino usposabljanja je treba pregledati in posodobiti tudi po:

9.2.1.1. pomembnem varnostnem incidentu,

9.2.1.2. pravnih ali pogodbenih spremembah,

9.2.1.3. organizacijskem prestrukturiranju ali migracijah sistemov.

9.3. Upravljanje različic in distribucija

9.3.1. Vsaka posodobitev mora vključevati:

9.3.1.1. številko različice in datum začetka veljavnosti,

9.3.1.2. povzetek sprememb,

9.3.1.3. odobritev generalnega direktorja,

9.3.1.4. arhiv vseh prejšnjih različic, ki se hrani najmanj tri leta.

9.4. Obveščanje zaposlenih

9.4.1. Posodobitve politike je treba sporočiti vsem zaposlenim, če so spremembe bistvene, pa je treba pridobiti tudi njihovo potrditev.

10. Povezane politike in povezave

10.1. Ta politika podpira naslednje:

10.1.1. P2S – Politika vlog in odgovornosti upravljanja: določa odgovornosti za usklajevanje usposabljanja in nadzor,

10.1.2. P3S – Politika sprejemljive uporabe (AUP): utrjuje pričakovanja glede vedenja, obravnavana v usposabljanju,

10.1.3. P4S – Politika nadzora dostopa: zagotavlja, da uporabniki razumejo pomen varnosti dostopa,

10.1.4. P7S – Politika uvajanja in prenehanja sodelovanja: vključuje usposabljanje v postopek uvajanja,

10.1.5. P30S – Politika odzivanja na incidente (P30): zagotavlja, da zaposleni znajo o incidentih poročati pravočasno in pravilno.

11. Referenčni standardi in okviri

11.1. ISO/IEC 27001

11.1.1. Klavzula 7.3 – zahteva, da organizacije zagotovijo, da so zaposleni seznanjeni s svojimi odgovornostmi in vplivom svojega ravnanja na varnost.

11.2. ISO/IEC 27002

11.2.1. Kontrola 6.3 – podrobneje določa pričakovanja glede obsega in izvajanja varnostnega usposabljanja.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AT-2 – zahteva usposabljanje za varnostno ozaveščenost za uporabnike z dostopom do sistemov.

11.3.2. AT-4 – obravnava usposabljanje na podlagi vlog in posledice neskladnosti.

11.4. EU GDPR

11.4.1. Člen 32 – zahteva varnostne ukrepe, vključno z usposabljanjem zaposlenih za varstvo osebnih podatkov.

11.4.2. Člen 39 – zahteva, da pooblaščene osebe za varstvo podatkov, kjer je to ustrezno, izvajajo nadzor nad ozaveščanjem in usposabljanjem.

11.5. Direktiva EU NIS2

11.5.1. Člen 21(2)(i) – zahteva stalne programe ozaveščanja in usposabljanja na področju kibernetske varnosti.

11.6. EU DORA

11.6.1. Člen 13 – zahteva, da finančni subjekti uvedejo izobraževanje in usposabljanje za vse zaposlene z odgovornostmi, povezanimi s sistemi IKT.

11.7. COBIT 2019

11.7.1. BAI08 – Upravljanje znanja: zagotavlja, da je osebje usposobljeno in ustrezno izobraženo.

11.7.2. DSS05 – Upravljanje varnostnih storitev: poudarja ozaveščanje kot ključni zaščitni ukrep.