					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P10S					Naslov dokumenta: **Politika čiste mize in zaslona**							
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	Klavzuli 7.2, 8	
ISO/IEC 27002:2022	Kontrola 7	
NIST SP 800-53 Rev.5	PE-2, AC-11	
Direktiva EU NIS2	Člen 21(2)(d)	
Uredba EU DORA	Člen 9(2)(f)	
COBIT 2019	DSS01.06, DSS05	
Uredba EU GDPR	Člen 32	

1. Namen

1.1 Ta politika določa zavezujoča pravila za vzdrževanje varnega delovnega okolja z zagotavljanjem, da so mize, delovne postaje in zasloni brez vidnih zaupnih informacij, kadar niso pod nadzorom.

1.2 Njen glavni namen je preprečiti nepooblaščen dostop do občutljivih informacij prek nenadzorovanih izpisov, odklenjenih zaslonov ali neustrezno odloženih izmenljivih medijev, tako v fizičnih pisarniških okoljih kot pri delu na daljavo.

1.3 Prakse čiste mize in zaslona, opredeljene v tej politiki, krepijo sposobnost organizacije za izpolnjevanje zahtev certifikacije ISO/IEC 27001 z zmanjševanjem tveganj nepotrebne izpostavljenosti. Te prakse strankam, partnerjem in presojevalcem dodatno potrjujejo, da informacijsko varnost obravnavamo resno tudi v okoljih z omejenimi viri.

1.4 Ta politika podpira kulturo odgovornosti in ozaveščenosti ter zagotavlja, da vse osebje, ne glede na vlogo ali tehnično strokovnost, razume svojo odgovornost za zaščito informacij podjetja in strank pred vidno izpostavljenostjo, krajo ali izgubo.

2. Obseg

2.1 Ta politika se uporablja za:

2.1.1 vse zaposlene, pogodbene izvajalce, praktikante in začasne delavce, ki uporabljajo delovne postaje, mize ali mobilne naprave, ki so v lasti podjetja ali so jim osebno dodeljene;

2.1.2 vse fizične lokacije, ki se uporabljajo za poslovne dejavnosti, vključno z namenskimi pisarnami, coworking prostori ter oddaljenimi oziroma domačimi delovnimi prostori;

2.1.3 vse digitalne naprave z možnostjo prikaza, vključno z namiznimi računalniki, prenosniki, tablicami in zunanjimi monitorji, ki se uporabljajo za poslovne namene.

2.2 Ta politika se razteza na vsa fizična ali digitalna sredstva, ki lahko prikazujejo, vsebujejo ali prenašajo občutljive informacije, vključno z:

2.2.1 tiskanimi evidencami ali ročno pisanimi zapiski;

2.2.2 USB-ključi, CD-ji in zunanjimi trdimi diski;

2.2.3 mobilnimi telefoni, ki se uporabljajo za poslovno sporočanje ali elektronsko pošto;

2.2.4 računalniškimi monitorji in projektorji, povezanimi z delovnimi sistemi.

2.3 Ta politika velja tudi zunaj rednega delovnega časa in med nestandardnimi dejavnostmi (npr. vzdrževanje po delovnem času ali delo v okviru odzivanja na incidente).

3. Cilji

3.1 Uveljaviti praktične in dosledne kontrole, ki zagotavljajo, da na mizah, zaslonih ali v skupnih prostorih niso izpostavljene občutljive informacije.

3.2 Zmanjšati tveganje nepooblaščenega dostopa iz notranjih virov (npr. nenamerni dostop drugih zaposlenih) in zunanjih groženj (npr. obiskovalci, čistilno osebje ali pogodbeni izvajalci).

3.3 Podpreti omejitve fizičnega in logičnega dostopa z zahtevo, da osebje aktivno varuje delovna gradiva in zaklene računalnike, kadar jih pusti brez nadzora.

3.4 Krepiti ozaveščenost osebja o varnih delovnih praksah ter zagotoviti preprosta in izvršljiva pravila, ki se uporabljajo pri vsakodnevnem delu ne glede na lokacijo dela.

3.5 Zagotoviti usklajenost s kontrolo 7.7 iz Priloge A standarda ISO/IEC 27001 ter s smernicami za njeno izvajanje po standardu ISO/IEC 27002 glede zahtev čiste mize in zaslona.

3.6 Zagotoviti, da lahko organizacija izkaže skrbno ravnanje in pripravljenost na presojo brez potrebe po infrastrukturi na ravni velikih podjetij.

4. Vloge in odgovornosti

4.1 Generalni direktor (GM)

4.1.1 Je lastnik te politike ter zagotavlja, da je politika ustrezno sporočena, razumljena in upoštevana s strani vseh zaposlenih in pogodbenih izvajalcev.

4.1.2 Odgovoren je za odobritev vseh izjem, obravnavo kršitev in nadzor nad usposabljanjem, povezanim z varnimi delovnimi praksami.

4.1.3 Mora izvajati redne preglede ali jih delegirati (najmanj četrtletno), da potrdi, da fizični in digitalni delovni prostori izpolnjujejo zahteve te politike.

4.2 Določeni član osebja (če je imenovan)

4.2.1 Lahko mu je dodeljena odgovornost za izvajanje tehničnih nastavitev (npr. nastavitev časovne omejitve zaslona) ali razdeljevanje pripomočkov za fizično shranjevanje (npr. zaklenljivih predalnikov).

4.2.2 Podpira GM s poročanjem o neskladnostih, podajanjem opomnikov glede varnosti delovnega prostora in spremljanjem odprave pomanjkljivosti, kadar so ugotovljene težave.

4.2.3 Pomaga zagotavljati, da imajo vsi zaposleni, kjer je to izvedljivo, dostop do ustreznih mehanizmov zaklepanja ali varnih prostorov za shranjevanje.

[... 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 GM mora to politiko pregledati najmanj enkrat letno in po katerem koli od naslednjih dogodkov:

9.1.1 uvedba novih pisarniških prostorov, naprav ali skupnih sistemov;

9.1.2 spremembe veljavnih pravnih zahtev ali zahtev za certifikacijo;

9.1.3 ugotovitve iz revizij, ocen tveganja ali varnostnih incidentov.

9.2 Vse vmesne posodobitve morajo biti sporočene vsem zaposlenim po elektronski pošti, pri čemer je zahtevana potrditev prejema in seznanitve.

9.3 Prejšnje različice te politike morajo biti varno shranjene in primerne za revizijsko sled, da je mogoče izkazati stalno usklajenost z ISO/IEC 27001 in povezanimi okviri.

10. Povezane politike in povezave

10.1 P2S – Politika vlog in odgovornosti upravljanja: pojasnjuje pooblastila GM za uveljavljanje in presojo ravnanja v fizičnih in digitalnih delovnih prostorih.

10.2 P4S – Politika nadzora dostopa: podpira tehnično izvajanje zaklepanja zaslona in praks varne prijave v delovno postajo.

10.3 P8S – Politika ozaveščanja in usposabljanja za informacijsko varnost: krepi vedenjsko usposabljanje, potrebno za skladnost s to politiko.

10.4 P17S – Politika varstva podatkov in zasebnosti: določa obveznosti glede ravnanja z osebnimi in občutljivimi podatki ter njihove zaščite v skladu z GDPR.

10.5 P30S – Politika odzivanja na incidente: določa okvir za eskalacijo in odziv, če kršitev povzroči izpostavljenost podatkov ali varnostni incident.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 7.2: zahteva, da so vsi zaposleni seznanjeni s svojimi varnostnimi odgovornostmi, vključno s fizičnim varovanjem.

11.1.2 Klavzula 8.1: operativne kontrole morajo zagotavljati ustrezne fizične in logične zaščitne ukrepe.

11.2 ISO/IEC 27002

11.2.1 Kontrola 7.7: podaja podrobne smernice za določitev, sporočanje in uveljavljanje zahtev čiste mize in zaslona.

11.3 NIST SP 800-53 Rev.5

11.3.1 PE-2: določa pričakovanja glede nadzora fizičnega dostopa, vključno z ravnanjem osebja v varovanih okoljih.

11.3.2 AC-11: zahteva funkcionalnost zaklepanja sej na delovnih postajah za preprečevanje nepooblaščenega vpogleda ali interakcije.

11.4 Uredba EU GDPR

11.4.1 Člen 32: zahteva, da organizacije osebne podatke varujejo s fizičnimi in tehničnimi varovalnimi ukrepi, vključno z delovnimi postajami in dokumenti.

11.5 Direktiva EU NIS2

11.5.1 Člen 21(2)(d): zahteva, da organizacije uvedejo politike fizičnega in logičnega dostopa na podlagi tveganj.

11.6 Uredba EU DORA

11.6.1 Člen 9(2)(f): zahteva politike varnosti IKT, vključno z varno higieno delovnega prostora, za subjekte finančnega sektorja in njihove dobavne verige.

11.7 COBIT 2019

11.7.1 DSS01.06: zahteva prakse zaščite sredstev, vključno s fizičnimi varnostnimi ukrepi nad delovnimi prostori in mediji.

11.7.2 DSS05.02: podpira uveljavljanje varnostnih praks končnih uporabnikov v operativnih okoljih.