					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P10					Naslov dokumenta: **Politika čiste mize in čistega 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	Klavzula 6.1.3, klavzula 8	načrt obravnave tveganj, operativno načrtovanje in kontrole za varne delovne prostore
ISO/IEC 27002:2022	Kontrola 7	vedenjske in okoljske kontrole za zaščito nenadzorovanih fizičnih informacij
NIST SP 800-53 Rev.5	PE-2, PS-7, MP-6, AC-11, CM-6, IA-5	fizični dostop, varnost pogodbenih izvajalcev, sanitizacija medijev, zaklep seje, konfiguracijske kontrole in kontrole avtentikatorjev
Uredba EU GDPR	Členi 5(1)(f), 32; uvodna izjava 39	celovitost podatkov, zaupnost in fizični varovalni ukrepi za podatke
Direktiva EU NIS2	Členi 21(2)(d), 21(3)	politike fizične varnosti, vedenje uporabnikov in preprečevanje uhajanja podatkov
Uredba EU DORA	Členi 5, 8, 9	notranje upravljanje, IKT in upravljanje incidentov, vključno s fizično varnostjo
COBIT 2019	DSS01, DSS05, MEA	upravljane operacije, varnostne storitve in spremljanje skladnosti

1. Namen

1.1 Ta politika določa obvezne kontrole za zaščito občutljivih informacij z zahtevo po varnem ravnanju s fizičnimi dokumenti, delovnimi postajami, zasloni in odstranljivimi mediji v pisarniških okoljih in skupnih delovnih prostorih.

1.2 Podpira kontrolo 7.7 Priloge A standarda ISO/IEC 27001 z uveljavljanjem vedenjskih in tehničnih praks, ki zmanjšujejo tveganje nepooblaščenega razkritja, kraje ali izgube podatkov zaradi nenadzorovanih ali vidnih informacij.

1.3 Ta politika krepi fizično in informacijsko varnost pri vsakodnevnem poslovanju ter podpira skladnost z veljavnimi zakonskimi, pogodbenimi in regulativnimi obveznostmi.

2. Področje uporabe

2.1 Ta politika velja za vse osebe, ki delujejo v fizičnih delovnih prostorih ali dostopajo do njih, vključno z:

2.1.1 zaposlenimi za nedoločen in določen čas,

2.1.2 pogodbenimi izvajalci, svetovalci, dobavitelji in praktikanti,

2.1.3 ponudniki storitev tretjih oseb in obiskovalci na lokaciji, ki imajo dostop do občutljivih informacij.

2.2 Zahteve veljajo v:

2.2.1 posameznih pisarnah, delovnih boksih in odprtih delovnih prostorih,

2.2.2 sejnih sobah in skupnih prostorih za sodelovanje,

2.2.3 območjih s tiskalniki, sprejemnih pultih in kopirnicah,

2.2.4 območjih, kjer se uporabljajo oddaljene delovne postaje ali skupni terminali.

2.3 Ta politika velja tudi za začasna ali hibridna delovna okolja (npr. hot-desking) ter javno dostopna okolja, kjer obstaja tveganje opazovanja čez ramo ali nenadzorovanih podatkov.

3. Cilji

3.1 Preprečiti nepooblaščen dostop do zaupnih, občutljivih ali reguliranih informacij, ki ostanejo izpostavljene v fizični ali digitalni obliki.

3.2 Spodbujati standardiziran profil tveganja na področju varnosti v vseh delovnih okoljih z uporabo fizičnih varovalnih ukrepov, konfiguracije delovnih postaj in vedenja končnih uporabnikov.

3.3 Zmanjšati tveganje kršitev zasebnosti, izgube intelektualne lastnine in uhajanja podatkov zaradi malomarnosti ali spregleda.

3.4 Vključiti ravnanje po načelih čiste mize in čistega zaslona v organizacijsko kulturo ter s tem podpreti operativno disciplino, preverljivost in regulatorno odgovornost.

3.5 Podpreti skladnost z ISO/IEC 27001, členom 32 GDPR, členom 21 Direktive EU NIS2 in drugimi zahtevami glede fizične varnosti, ki se nanašajo na kritične ali osebne podatke.

4. Vloge in odgovornosti

4.1 Najvišje vodstvo

4.1.1 Potrdi to politiko in spodbuja kulturo varnostnega zavedanja v vseh poslovnih enotah.

4.1.2 Zagotovi ustrezne vire za izvajanje politike, kampanje ozaveščanja in mehanizme fizičnih kontrol.

4.2 Vodja informacijske varnosti / vodja ISMS

4.2.1 Je lastnik te politike in zagotavlja njeno usklajenost z ISO/IEC 27001:2022, revizijskimi zahtevami in strategijami obravnave tveganj.

4.2.2 Razvija programe ozaveščanja in kontrole za dosledno izvajanje v vseh objektih in hibridnih oblikah dela.

4.2.3 Usklajuje delo s službo za upravljanje objektov in IT, da so vzpostavljeni ustrezni fizični varovalni ukrepi.

[... 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 Načrt pregledov politike

9.1.1 Ta politika se pregleda:

9.1.1.1 najmanj enkrat letno,

9.1.1.2 po vsaki neskladnosti, ugotovljeni pri presoji, ki je povezana z izpostavljenostjo delovnega prostora ali zaslona,

9.1.1.3 po fizičnem ali okoljskem incidentu (npr. kraja naprave, nedovoljeno sledenje pri vstopu, opazovanje),

9.1.1.4 ob uvedbi novih pisarniških postavitev, politik upravljanja objektov ali modelov delovnih prostorov (npr. hot-desking, oddaljena vozlišča).

9.2 Odgovorni lastniki

9.2.1 Lastnik politike je vodja informacijske varnosti ali imenovani vodja ISMS.

9.2.2 V postopek pregleda morajo biti vključeni:

9.2.2.1 ekipe za upravljanje objektov in korporativno varnost,

9.2.2.2 IT in infrastruktura za uveljavljanje ukrepov, povezanih z napravami,

9.2.2.3 kadrovska služba (HR) in pravna služba za uveljavljanje vedenjskih pravil in usklajenost disciplinskih ukrepov.

9.2.3 Vse posodobitve politike morajo biti verzionirane, odobrene s strani usmerjevalnega odbora ISMS ter ponovno posredovane s ponovno potrditvijo, kjer je to zahtevano.

9.3 Sporočanje sprememb

9.3.1 Uporabniki morajo biti o pomembnih posodobitvah obveščeni prek:

9.3.1.1 intranetnega središča politik ali portala,

9.3.1.2 ciljno usmerjene elektronske pošte,

9.3.1.3 obnovitvenih uvajalnih vsebin in četrtletnih obvestil,

9.3.1.4 obveznih pozivov k potrditvi za vse nove kritične klavzule glede uveljavljanja.

10. Povezane politike in povezave

10.1 Ta politika je usklajena z naslednjimi politikami in jih podpira:

10.1.1 P1 – Politika informacijske varnosti: določa pričakovanja glede vedenja uporabnikov in fizične varnosti, ki so temelj te politike.

10.1.2 P3 – Politika sprejemljive uporabe (AUP): obravnava odgovornost uporabnikov za zaščito podatkov in sistemov, vključno s fizičnimi okolji.

10.1.3 P6 – Politika obvladovanja tveganj: vključuje tveganja fizičnih delovnih prostorov v analizo informacijskih tveganj na ravni celotne organizacije.

10.1.4 P12 – Politika upravljanja sredstev: podpira sledenje napravam in medijem, puščenim na mizah, ter varno ravnanje z njimi.

10.1.5 P13 – Politika klasifikacije in označevanja podatkov: povezuje izvajanje čiste mize s fizičnimi dokumenti, označenimi kot zaupno ali interno.

10.1.6 P14 – Politika hrambe in odstranjevanja podatkov: usmerja hrambo fizičnih dokumentov, uničevanje in ravnanje z zbiralniki.

10.1.7 P22 – Politika beleženja in spremljanja: lahko se uporablja za spremljanje stanja zaklepa delovnih postaj, časa nedejavnosti ali kamer v delovnih prostorih, kjer je to dovoljeno.

10.2 Te povezane politike vzpostavljajo celovito varnostno kulturo, ki združuje ozaveščenost uporabnikov, fizične varovalne ukrepe in odgovornost za zagotavljanje odpornih delovnih prostorov.

11. Referenčni standardi in okviri

11.1 Ta politika je usklajena z globalno priznanimi standardi in pravnimi zahtevami, ki določajo zaščito občutljivih informacij v fizičnih okoljih in prek vedenja uporabnikov.

11.2 ISO/IEC 27001

11.2.1 Klavzula 6.1.3 – načrt obravnave tveganj: podpira izvajanje kontrol za zmanjševanje fizičnih in okoljskih tveganj, vključno s tveganji, povezanimi z vedenjem uporabnikov v odprtih delovnih prostorih.

11.2.2 Klavzula 8.1 – operativno načrtovanje in kontrola: določa operativne varovalne ukrepe za upravljanje varnih delovnih prostorov in uporabe opreme.

11.3 ISO/IEC 27002:2022 – Kontrola 7

11.3.1 Ta kontrola zahteva vedenjske in okoljske zaščitne ukrepe za preprečevanje nepooblaščenega dostopa do informacij prek nenadzorovanih medijev, zaslonov ali tiskanih gradiv. Ta politika uveljavlja urejenost fizičnih delovnih prostorov, uporabo zaklepa zaslona in odstranjevanje občutljivih dokumentov.

11.4 NIST SP 800-53 Rev.5

11.4.1 PE-2 (odobritve fizičnega dostopa): povezan je z omejitvami delovnih prostorov in uveljavljanjem zaklenjene hrambe v okoljih z visokim tveganjem.

11.4.2 PS-7 (varnost zunanjega osebja): uporablja se prek zahtev čiste mize in čistega zaslona, razširjenih na pogodbene izvajalce in uporabnike tretjih oseb.

11.4.3 MP-6 (sanitizacija medijev) in AC-11 (zaklep seje): izvajata se prek postopkov varne odstranitve in obveznih časovnikov zaklepa zaslona.

11.4.4 CM-6 (nastavitve konfiguracije) in IA-5 (upravljanje avtentikatorjev): podpirata tehnično uveljavljanje zaklepanja zaslona in nadzora sej na končnih točkah.

11.5 Uredba EU GDPR (2016/679)

11.5.1 Člen 5(1)(f): uveljavlja celovitost in zaupnost osebnih podatkov, vključno z zaščito pred fizično izpostavljenostjo ali vpogledom nepooblaščenih oseb.

11.5.2 Člen 32 – varnost obdelave: zahteva ustrezne fizične in organizacijske ukrepe za zaščito osebnih podatkov pred nenamernim ali nezakonitim uničenjem, izgubo ali nepooblaščenim razkritjem, kar se dosega s kontrolami čiste mize in čistega zaslona.

11.5.3 Uvodna izjava 39: zahteva omejitev dostopa do osebnih podatkov na pooblaščene posameznike, kar vključuje tudi njihovo zaščito v fizični obliki, kadar niso pod nadzorom.

11.6 Direktiva EU NIS2 (2022/2555)

11.6.1 Člen 21(2)(d): zahteva politike in postopke v zvezi s fizično in okoljsko varnostjo, vključno z zaščito informacij na ravni delovnega mesta.

11.6.2 Člen 21(3): spodbuja varnostno kulturo, ki vključuje ustrezno vedenje uporabnikov, ozaveščanje in preprečevanje nenamernega uhajanja podatkov, kar podpirajo vedenjske kontrole te politike.

11.7 Uredba EU DORA (2022/2554)

11.7.1 Člen 5 – notranje upravljanje in kontrola: zahteva, da se vsa tveganja, povezana z IKT, vključno s človeškimi in okoljskimi grožnjami, upravljajo z izvršljivimi politikami.

11.7.2 Člen 8 – upravljanje tveganj IKT: zahteva varovalne ukrepe v digitalnem in fizičnem okolju ter zagotavlja, da uporabniki na daljavo, v podružnicah in na lokaciji ne ustvarjajo neupravljane izpostavljenosti.

11.7.3 Člen 9 – upravljanje incidentov: zahteva, da se okoljske ali vedenjske opustitve, ki povzročijo izpostavljenost podatkov, beležijo, razvrščajo in obravnavajo z ustreznimi korektivnimi ukrepi.

11.8 COBIT 2019

11.8.1 DSS01 – upravljane operacije: zagotavlja operativno disciplino pri zaščiti fizičnih delovnih prostorov in sistemov s ponovljivimi kontrolami.

11.8.2 DSS05 – upravljane varnostne storitve: podpira zaščito podatkov, naprav in dostopnih končnih točk z vedenjsko pogojenim izvajanjem, kot so prakse čiste mize.

11.8.3 MEA03 – spremljanje, vrednotenje in presoja skladnosti: spodbuja presojo fizičnih varovalnih ukrepov in sprejetosti politike v vsakodnevnih poslovnih praksah.