					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P10					Naziv dokumenta: **Politika čistog radnog stola i zaključanog zaslona**							
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 sa standardima i propisima

Standard/propis	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 6.1.3, Točka 8	plan obrade rizika, operativno planiranje i kontrola za sigurna radna okruženja
ISO/IEC 27002:2022	Kontrola 7	kontrole ponašanja i okolišne kontrole za zaštitu fizičkih informacija ostavljenih bez nadzora
NIST SP 800-53 Rev.5	PE-2, PS-7, MP-6, AC-11, CM-6, IA-5	fizički pristup, sigurnost ugovornih izvođača, zbrinjavanje medija, zaključavanje sesije, konfiguracijske kontrole i kontrole autentifikatora
GDPR EU	Članci 5(1)(f), 32; uvodna izjava 39	cjelovitost podataka, povjerljivost i fizičke zaštitne mjere za podatke
Direktiva EU NIS2	Članci 21(2)(d), 21(3)	politike fizičke sigurnosti, ponašanja korisnika i sprječavanja curenja podataka
Uredba EU DORA	Članci 5, 8, 9	interno upravljanje, IKT i upravljanje incidentima koji uključuju fizičku sigurnost
COBIT 2019	DSS01, DSS05, MEA	upravljane operacije, sigurnosne usluge i praćenje usklađenosti

1. Svrha

1.1 Ova politika uspostavlja obvezne kontrole za zaštitu osjetljivih informacija zahtijevajući sigurno postupanje s fizičkim dokumentima, radnim stanicama, zaslonima i prijenosnim medijima u uredskim i dijeljenim radnim okruženjima.

1.2 Ova politika podupire kontrolu 7.7 Dodatka A norme ISO/IEC 27001 primjenom kontrola ponašanja i tehničkih praksi koje ublažavaju rizik od neovlaštenog otkrivanja, krađe ili gubitka podataka zbog informacija ostavljenih bez nadzora ili vidljivih neovlaštenim osobama.

1.3 Ova politika jača fizičku i informacijsku sigurnost u svakodnevnom poslovanju te podupire usklađenost s primjenjivim zakonskim, ugovornim i regulatornim obvezama.

2. Opseg

2.1 Ova politika primjenjuje se na sve osoblje koje radi u fizičkim radnim prostorima ili im pristupa, uključujući:

2.1.1 stalno i privremeno osoblje

2.1.2 ugovorne izvođače, konzultante, dobavljače i vježbenike

2.1.3 pružatelje usluga trećih strana i posjetitelje na lokaciji koji imaju pristup osjetljivim informacijama

2.2 Zahtjevi se primjenjuju u:

2.2.1 pojedinačnim uredima, boksovima i otvorenim radnim prostorima

2.2.2 sobama za sastanke i zajedničkim prostorima za suradnju

2.2.3 prostorima s pisačima, recepcijama i prostorijama za kopiranje

2.2.4 područjima u kojima se koriste udaljene radne stanice ili dijeljeni kiosci

2.3 Ova politika primjenjuje se i na privremena ili hibridna radna okruženja, uključujući hot-desking, te na javno dostupna okruženja u kojima postoji rizik od promatranja preko ramena ili ostavljanja podataka bez nadzora.

3. Ciljevi

3.1 Spriječiti neovlašteni pristup povjerljivim, osjetljivim ili reguliranim informacijama ostavljenima izloženima u fizičkom ili digitalnom obliku.

3.2 Promicati standardizirani sigurnosni profil u svim radnim okruženjima primjenom fizičkih zaštitnih mjera, konfiguracije radnih stanica i odgovarajućeg ponašanja krajnjih korisnika.

3.3 Smanjiti rizik od povreda privatnosti, gubitka intelektualnog vlasništva i eksfiltracije podataka uzrokovanih nepažnjom ili propustom.

3.4 Ugraditi ponašanje čistog radnog stola i zaključanog zaslona u organizacijsku kulturu radi potpore operativnoj disciplini, mogućnosti revizije i dokazivosti usklađenosti.

3.5 Poduprijeti usklađenost s normom ISO/IEC 27001, člankom 32 GDPR-a, člankom 21 Direktive EU NIS2 i drugim zahtjevima fizičke sigurnosti relevantnima za kritične ili osobne podatke.

4. Uloge i odgovornosti

4.1 Izvršno rukovodstvo

4.1.1 Odobrava ovu politiku i promiče kulturu sigurnosne osviještenosti u svim poslovnim jedinicama.

4.1.2 Dodjeljuje odgovarajuće resurse za provedbu politike, kampanje podizanja svijesti i mehanizme fizičke zaštite.

4.2 Glavni direktor informacijske sigurnosti (CISO) / voditelj ISMS-a

4.2.1 Vlasnik je ove politike i osigurava njezinu usklađenost s normom ISO/IEC 27001:2022, revizijskim zahtjevima i strategijama obrade rizika.

4.2.2 Razvija programe podizanja svijesti i kontrole radi osiguravanja dosljedne provedbe na svim lokacijama i u hibridnim radnim okruženjima.

4.2.3 Koordinira s timovima za upravljanje objektima i IT-om radi osiguravanja odgovarajućih fizičkih zaštitnih mjera.

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Zahtjevi za pregled i ažuriranje

9.1 Raspored pregleda politike

9.1.1 Ova politika mora se pregledati:

9.1.1.1 najmanje jednom godišnje

9.1.1.2 nakon svake nesukladnosti utvrđene revizijom povezane s izloženošću radnog prostora ili zaslona

9.1.1.3 nakon fizičkog ili okolišnog incidenta, primjerice krađe uređaja, neovlaštenog ulaska uz praćenje ovlaštene osobe ili nadzora

9.1.1.4 pri uvođenju novih uredskih rasporeda, politika upravljanja objektima ili modela radnog prostora, primjerice hot-deskinga ili udaljenih čvorišta

9.2 Odgovorni vlasnici

9.2.1 Vlasnik politike je glavni direktor informacijske sigurnosti (CISO) ili imenovani voditelj ISMS-a.

9.2.2 Postupak pregleda mora uključivati:

9.2.2.1 timove za upravljanje objektima i korporativnu sigurnost

9.2.2.2 IT i infrastrukturu za provedbu kontrola povezanih s uređajima

9.2.2.3 ljudske resurse (HR) i pravne poslove radi provedbe očekivanog ponašanja i usklađivanja stegovnih mjera

9.2.3 Sve izmjene politike moraju biti pod verzijskom kontrolom, odobrene od strane Upravljačkog odbora ISMS-a i ponovno distribuirane uz ponovnu potvrdu upoznatosti, kada je to potrebno.

9.3 Komunikacija promjena

9.3.1 Korisnici moraju biti obaviješteni o značajnim ažuriranjima putem:

9.3.1.1 intranetskog središta za politike ili portala

9.3.1.2 ciljanih komunikacija elektroničkom poštom

9.3.1.3 obnovnih sadržaja pri uvođenju u posao i tromjesečnih brifinga

9.3.1.4 obveznih zahtjeva za potvrdu upoznatosti za sve nove kritične odredbe o provedbi

10. Povezane politike i poveznice

10.1 Ova politika usklađena je sa sljedećim politikama i podupire ih:

10.1.1 P1 – Politika informacijske sigurnosti: uspostavlja očekivanja u vezi s ponašanjem korisnika i fizičkom sigurnošću koja su temelj ove politike.

10.1.2 P3 – Politika prihvatljive uporabe: uređuje odgovornost korisnika za zaštitu podataka i sustava, uključujući fizička okruženja.

10.1.3 P6 – Politika upravljanja rizicima: uključuje rizike fizičkog radnog prostora kao dio organizacijske analize informacijskih rizika.

10.1.4 P12 – Politika upravljanja imovinom: podupire praćenje i sigurno postupanje s uređajima i medijima ostavljenima na radnim stolovima.

10.1.5 P13 – Politika klasifikacije podataka i označavanja: povezuje provedbu čistog radnog stola s fizičkim dokumentima označenima kao povjerljivi ili za internu uporabu.

10.1.6 P14 – Politika zadržavanja i zbrinjavanja podataka: daje smjernice za zadržavanje fizičkih dokumenata, usitnjavanje i postupanje sa spremnicima.

10.1.7 P22 – Politika revizijskog bilježenja i praćenja: može se koristiti za praćenje statusa zaključavanja radnih stanica, vremena neaktivnosti ili snimki kamera radnog prostora, gdje je to dopušteno.

10.2 Ove povezane politike uspostavljaju integriranu sigurnosnu kulturu koja povezuje svijest korisnika, fizičke zaštitne mjere i odgovornost radi osiguravanja otpornih radnih prostora.

11. Referentni standardi i okviri

11.1 Ova politika usklađena je s globalno priznatim standardima i pravnim zahtjevima koji nalažu zaštitu osjetljivih informacija u fizičkim okruženjima i kroz ponašanje korisnika.

11.2 ISO/IEC 27001

11.2.1 Točka 6.1.3 – Plan obrade rizika: podupire provedbu kontrola za ublažavanje fizičkih i okolišnih rizika, uključujući one povezane s ponašanjem korisnika u otvorenim radnim prostorima.

11.2.2 Točka 8.1 – Operativno planiranje i kontrola: uspostavlja operativne zaštitne mjere za upravljanje sigurnim radnim prostorima i uporabom opreme.

11.3 ISO/IEC 27002:2022 – Kontrola 7

11.3.1 Ova kontrola zahtijeva kontrole ponašanja i okolišne kontrole radi sprječavanja neovlaštenog pristupa informacijama putem medija, zaslona ili tiskanih materijala ostavljenih bez nadzora. Ova politika propisuje urednost fizičkog radnog prostora, uporabu zaključavanja zaslona i zbrinjavanje osjetljivih dokumenata.

11.4 NIST SP 800-53 Rev.5

11.4.1 PE-2 (Ovlaštenja za fizički pristup): povezan je s ograničenjima radnog prostora i provedbom zaključane pohrane u okruženjima visokog rizika.

11.4.2 PS-7 (Sigurnost vanjskog osoblja): primjenjuje se kroz zahtjeve čistog radnog stola i zaključanog zaslona proširene na ugovorne izvođače i korisnike trećih strana.

11.4.3 MP-6 (Sanitizacija medija) i AC-11 (Zaključavanje sesije): provode se putem postupaka sigurnog zbrinjavanja i obveznih vremenskih postavki zaključavanja zaslona.

11.4.4 CM-6 (Postavke konfiguracije) i IA-5 (Upravljanje autentifikatorima): podupiru tehničku provedbu zaključavanja zaslona i kontrole sesije na krajnjim uređajima.

11.5 GDPR EU (2016/679)

11.5.1 Članak 5(1)(f): zahtijeva cjelovitost i povjerljivost osobnih podataka, uključujući zaštitu od fizičke izloženosti ili uvida od strane neovlaštenih osoba.

11.5.2 Članak 32 – Sigurnost obrade: zahtijeva odgovarajuće fizičke i organizacijske mjere za zaštitu osobnih podataka od slučajnog ili nezakonitog uništenja, gubitka ili neovlaštenog otkrivanja, što se postiže kontrolama radnog stola i zaslona.

11.5.3 Uvodna izjava 39: zahtijeva ograničavanje pristupa osobnim podacima na ovlaštene pojedince, što uključuje i njihovu zaštitu u fizičkom obliku kada su ostavljeni bez nadzora.

11.6 Direktiva EU NIS2 (2022/2555)

11.6.1 Članak 21(2)(d): zahtijeva politike i postupke povezane s fizičkom sigurnošću i sigurnošću okoline, uključujući zaštitu informacijske sigurnosti na razini radnog mjesta.

11.6.2 Članak 21(3): potiče sigurnosnu kulturu koja uključuje odgovarajuće ponašanje korisnika, podizanje svijesti i sprječavanje nenamjernog curenja podataka, što je podržano kontrolama ponašanja iz ove politike.

11.7 Uredba EU DORA (2022/2554)

11.7.1 Članak 5 – Interno upravljanje i kontrola: zahtijeva da se svim rizicima povezanima s IKT-om, uključujući ljudske i okolišne prijetnje, upravlja putem provedivih politika.

11.7.2 Članak 8 – Upravljanje IKT rizicima: zahtijeva zaštitne mjere u digitalnom i fizičkom kontekstu, osiguravajući da korisnici na daljinu, u podružnicama i u vlastitim prostorijama ne stvaraju izloženost kojom se ne upravlja.

11.7.3 Članak 9 – Upravljanje incidentima: zahtijeva da se okolišni ili ponašajni propusti koji rezultiraju izloženošću podataka evidentiraju, klasificiraju i rješavaju odgovarajućim korektivnim radnjama.

11.8 COBIT 2019

11.8.1 DSS01 – Upravljane operacije: osigurava operativnu disciplinu u zaštiti fizičkih radnih prostora i sustava kroz ponovljive kontrole.

11.8.2 DSS05 – Upravljane sigurnosne usluge: podupire zaštitu podataka, uređaja i pristupnih krajnjih točaka kroz provedbu zahtjeva temeljenih na ponašanju, kao što su prakse čistog radnog stola.

11.8.3 MEA03 – Praćenje, vrednovanje i procjena usklađenosti: potiče reviziju fizičkih zaštitnih mjera i primjene politike u svakodnevnoj poslovnoj praksi.