| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Ovdje unesite naziv registrirane pravne osobe | | | | | | | |
| Broj dokumenta:<br>P10S | | | | | Naziv dokumenta:<br>**Politika čistog stola i zaključanog zaslona** | | | | | | | |
| Verzija:<br>1.0 | | Datum stupanja na snagu:<br>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/regulativa | Točka/članak | Napomena |
|---|---|---|
| ISO/IEC 27001:2022 | Točke 7.2, 8 | |
| ISO/IEC 27002:2022 | Kontrola 7 | |
| NIST SP 800-53 Rev.5 | PE-2, AC-11 | |
| EU NIS2 | Članak 21(2)(d) | |
| EU DORA | Članak 9(2)(f) | |
| COBIT 2019 | DSS01.06, DSS05 | |
| GDPR EU | Članak 32 | |

## 1. Svrha

1.1 Ova politika utvrđuje obvezujuće zahtjeve za održavanje sigurnog radnog okruženja tako da stolovi, radne stanice i zasloni ne sadrže vidljive povjerljive informacije kada su bez nadzora.

1.2 Svrha ove politike jest spriječiti neovlašteni pristup osjetljivim informacijama putem ostavljenih ispisa, otključanih zaslona ili nepravilno odloženih prijenosnih medija, u fizičkim uredskim okruženjima i na lokacijama rada na daljinu.

1.3 Prakse čistog stola i zaključanog zaslona definirane ovom politikom jačaju sposobnost organizacije da ispuni zahtjeve za certifikaciju prema normi ISO/IEC 27001 smanjenjem rizika od izloženosti koji se mogu spriječiti. Te prakse također potvrđuju klijentima, partnerima i revizorima da organizacija informacijskoj sigurnosti pristupa ozbiljno, uključujući i okruženja s ograničenim resursima.

1.4 Ova politika podupire kulturu odgovornosti i svijesti te osigurava da svo osoblje, neovisno o ulozi ili tehničkoj stručnosti, razumije svoju odgovornost za zaštitu informacija organizacije i klijenata od vizualne izloženosti, krađe ili gubitka.

## 2. Opseg

**2.1 Ova politika primjenjuje se na:**

2.1.1 sve zaposlenike, ugovorne suradnike, vježbenike i privremeno osoblje koje koristi radne stanice, stolove ili mobilne uređaje u vlasništvu organizacije ili osobno dodijeljene za rad

2.1.2 sve fizičke lokacije koje se koriste za poslovne aktivnosti, uključujući namjenske urede, dijeljene radne prostore i udaljene/kućne radne prostore

2.1.3 sve digitalne uređaje s mogućnošću prikaza, uključujući stolna računala, prijenosna računala, tablete i vanjske monitore koji se koriste u poslovne svrhe

**2.2 Ova politika obuhvaća svu fizičku i digitalnu imovinu koja može prikazivati, sadržavati ili prenositi osjetljive informacije, uključujući:**

2.2.1 ispisane zapise ili rukom pisane bilješke

2.2.2 USB memorije, CD-ove i vanjske tvrde diskove

2.2.3 mobilne telefone koji se koriste za poslovne poruke ili e-poštu

2.2.4 računalne monitore i projektore povezane s radnim sustavima

2.3 Ova politika ostaje primjenjiva i izvan redovnog radnog vremena te tijekom nestandardnih aktivnosti, primjerice održavanja nakon radnog vremena ili rada u sklopu odgovora na incidente.

**3. Ciljevi**

3.1 Uspostaviti praktične i dosljedne kontrole kojima se osigurava da osjetljive informacije ne ostanu izložene na stolovima, zaslonima ili u zajedničkim prostorima.

3.2 Smanjiti rizik od neovlaštenog pristupa, kako iz unutarnjih izvora (npr. nenamjerni pristup drugih zaposlenika) tako i od vanjskih prijetnji (npr. posjetitelji, osoblje za čišćenje ili ugovorni suradnici).

3.3 Poduprijeti ograničenja fizičkog i logičkog pristupa tako da se od osoblja zahtijeva aktivno osiguravanje radnih materijala i zaključavanje računala kada ih ostavljaju bez nadzora.

3.4 Jačati svijest osoblja o sigurnim radnim praksama i osigurati jednostavna, provediva pravila primjenjiva u svakodnevnom radu, neovisno o lokaciji rada.

3.5 Osigurati usklađenost s kontrolom 7.7 iz Dodatka A norme ISO/IEC 27001 i pripadajućim smjernicama za provedbu iz norme ISO/IEC 27002 za zahtjeve čistog stola i zaključanog zaslona.

3.6 Osigurati da organizacija može dokazati dužnu pažnju i spremnost za reviziju bez potrebe za infrastrukturom razine velikih poduzeća.

**4. Uloge i odgovornosti**

**4.1 glavni direktor (GM)**

4.1.1 Odgovoran je za ovu politiku i osigurava da bude pravilno priopćena, razumljiva te da je se pridržavaju svi zaposlenici i ugovorni suradnici.

4.1.2 Odgovoran je za odobravanje svih iznimki, postupanje u slučaju kršenja i nadzor nad osposobljavanjem povezanim sa sigurnim radnim praksama.

4.1.3 Mora provoditi redovite provjere ili ih delegirati, najmanje tromjesečno, kako bi potvrdio da fizički i digitalni radni prostori ispunjavaju zahtjeve iz ove politike.

**4.2 imenovana osoba iz osoblja (ako je određena)**

4.2.1 Može joj se dodijeliti odgovornost za provedbu tehničkih postavki (npr. postavki isteka vremena zaslona) ili distribuciju fizičkih sredstava za pohranu (npr. ladica s bravom).

4.2.2 Podupire GM-a prijavljivanjem neusklađenosti, upućivanjem podsjetnika o sigurnosti radnog prostora i praćenjem korektivnih mjera kada se utvrde problemi.

4.2.3 Pomaže osigurati da svi zaposlenici, gdje je to izvedivo, imaju pristup odgovarajućim mehanizmima zaključavanja ili sigurnim prostorima za pohranu.

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

**9. Zahtjevi za pregled i ažuriranje**

**9.1 GM mora pregledati ovu politiku najmanje jednom godišnje i nakon bilo kojeg od sljedećih događaja:**

9.1.1 uvođenja novih uredskih prostora, uređaja ili dijeljenih sustava

9.1.2 promjena primjenjivih pravnih zahtjeva ili zahtjeva za certifikaciju

9.1.3 nalaza revizije, procjena rizika ili sigurnosnih incidenata

9.2 Privremena ažuriranja moraju se priopćiti svim zaposlenicima putem e-pošte, uz obveznu potvrdu upoznatosti.

9.3 Prethodne verzije ove politike moraju se sigurno pohraniti i biti dostupne za reviziju kako bi se dokazala trajna usklađenost s normom ISO/IEC 27001 i povezanim okvirima.

**10. Povezane politike i upućivanja**

10.1 P2S – Politika uloga i odgovornosti u upravljanju: pojašnjava ovlasti GM-a za provedbu i reviziju postupanja u fizičkim i digitalnim radnim prostorima.

10.2 P4S – Politika kontrole pristupa: podupire tehničku provedbu zaključavanja zaslona i sigurnih praksi prijave na radne stanice.

10.3 P8S – Politika podizanja svijesti i osposobljavanja o informacijskoj sigurnosti: jača osposobljavanje u području ponašanja potrebnog za usklađenost s ovom politikom.

10.4 P17S – Politika zaštite podataka i privatnosti: definira obveze za postupanje s osobnim i osjetljivim podacima te njihovu zaštitu u skladu s GDPR-om.

10.5 P30S – Politika odgovora na incidente: pruža okvir za eskalaciju i odgovor ako kršenje rezultira izloženošću podataka ili povredom.

## 11. Referentni standardi i okviri

### 11.1 ISO/IEC 27001

11.1.1 Točka 7.2: zahtijeva da sve osoblje bude svjesno sigurnosnih odgovornosti, uključujući fizičke zaštitne mjere.

11.1.2 Točka 8.1: operativne kontrole moraju osigurati odgovarajuće fizičke i logičke zaštitne mjere.

### 11.2 ISO/IEC 27002

11.2.1 Kontrola 7.7: daje detaljne smjernice za uspostavu, priopćavanje i provedbu zahtjeva čistog stola i zaključanog zaslona.

### 11.3 NIST SP 800-53 Rev.5

11.3.1 PE-2: uspostavlja očekivanja kontrole fizičkog pristupa, uključujući postupanje osoblja u sigurnim okruženjima.

11.3.2 AC-11: zahtijeva funkcionalnost zaključavanja sesije na radnim stanicama radi sprječavanja neovlaštenog pregleda ili interakcije.

### 11.4 GDPR EU

11.4.1 Članak 32: zahtijeva da organizacije štite osobne podatke primjenom fizičkih i tehničkih zaštitnih mjera, uključujući radne stanice i dokumente.

### 11.5 Direktiva EU NIS2

11.5.1 Članak 21(2)(d): zahtijeva da organizacije provedu politike fizičkog i logičkog pristupa utemeljene na riziku.

### 11.6 Uredba EU DORA

11.6.1 Članak 9(2)(f): zahtijeva politike sigurnosti IKT-a, uključujući sigurnu higijenu radnog prostora, za subjekte financijskog sektora i njihove opskrbne lance.

### 11.7 COBIT 2019

11.7.1 DSS01.06: zahtijeva prakse zaštite imovine, uključujući fizičke kontrole nad radnim prostorima i medijima.

11.7.2 DSS05.02: podupire provedbu sigurnosnih praksi krajnjih korisnika u svim operativnim okruženjima.