					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P10S					Názov dokumentu: **Politika čistého pracovného stola a uzamknutej obrazovky**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Štandard		Postup		Formulár		Register		Iné	

História revízií				
Číslo revízie	**Dátum revízie**	**Zmeny**	**Preskúmal**	**Vlastník procesu**

Schválenia			
Meno	**Pozícia**	**Dátum**	**Podpis**

Súlad s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitoly 7.2, 8	
ISO/IEC 27002:2022	Kontrola 7	
NIST SP 800-53 Rev.5	PE-2, AC-11	
Smernica EÚ NIS2	Článok 21(2)(d)	
Nariadenie EÚ DORA	Článok 9(2)(f)	
COBIT 2019	DSS01.06, DSS05	
Nariadenie EÚ GDPR	Článok 32	

1. Účel

1.1 Táto politika stanovuje záväzné pravidlá na udržiavanie bezpečného pracovného prostredia tým, že zabezpečuje, aby na pracovných stoloch, pracovných staniciach a obrazovkách neboli počas neprítomnosti používateľa viditeľné dôverné informácie.

1.2 Jej hlavným účelom je predchádzať neoprávnenému prístupu k citlivým informáciám prostredníctvom ponechaných výtlačkov bez dozoru, neuzamknutých obrazoviek alebo nesprávne uložených vymeniteľných médií, a to vo fyzických kancelárskych priestoroch aj pri práci na diaľku.

1.3 Postupy čistého pracovného stola a uzamknutej obrazovky definované v tejto politike posilňujú schopnosť organizácie plniť požiadavky certifikácie podľa ISO/IEC 27001 tým, že minimalizujú riziko zbytočného sprístupnenia informácií. Tieto postupy zároveň poskytujú zákazníkom, partnerom a audítorom uistenie, že informačnú bezpečnosť berieme vážne aj v prostredí s obmedzenými zdrojmi.

1.4 Táto politika podporuje kultúru zodpovednosti a povedomia a zabezpečuje, aby všetci pracovníci bez ohľadu na rolu alebo technickú odbornosť rozumeli svojej povinnosti chrániť informácie organizácie a informácie zákazníkov pred vizuálnym odhalením, odcudzením alebo stratou.

2. Rozsah

2.1 Táto politika sa vzťahuje na:

2.1.1 všetkých zamestnancov, zmluvných pracovníkov, stážistov a dočasných pracovníkov, ktorí používajú pracovné stanice, pracovné stoly alebo mobilné zariadenia vo vlastníctve spoločnosti alebo im osobne pridelené,

2.1.2 všetky fyzické lokality využívané na činnosť organizácie vrátane vyhradených kancelárií, coworkingových priestorov a pracovísk doma alebo pri práci na diaľku,

2.1.3 všetky digitálne zariadenia so zobrazovacími schopnosťami vrátane stolových počítačov, notebookov, tabletov a externých monitorov používaných na pracovné účely.

2.2 Politika sa vzťahuje aj na akékoľvek fyzické alebo digitálne aktívum, ktoré môže zobrazovať, obsahovať alebo prenášať citlivé informácie, vrátane:

2.2.1 tlačených záznamov alebo rukou písaných poznámok,

2.2.2 USB kľúčov, CD a externých pevných diskov,

2.2.3 mobilných telefónov používaných na pracovnú komunikáciu alebo e-mail,

2.2.4 monitorov a projektorov pripojených k pracovným systémom.

2.3 Táto politika sa uplatňuje aj mimo bežného pracovného času a počas neštandardných prevádzkových činností (napr. údržba po pracovnom čase alebo činnosti v rámci reakcie na núdzové situácie).

3. Ciele

3.1 Uplatňovať praktické a konzistentné kontroly, ktoré zabezpečia, že na pracovných stoloch, obrazovkách alebo v spoločných priestoroch nezostanú voľne prístupné žiadne citlivé informácie.

3.2 Minimalizovať riziko neoprávneného prístupu zo strany interných zdrojov (napr. neúmyselný prístup iných zamestnancov) aj externých hrozieb (napr. návštevníci, upratovací personál alebo zmluvní dodávatelia a poskytovatelia služieb tretích strán).

3.3 Podporiť obmedzenia fyzického a logického prístupu tým, že sa od pracovníkov vyžaduje aktívne zabezpečenie pracovných materiálov a uzamknutie počítačov počas neprítomnosti.

3.4 Posilňovať povedomie pracovníkov o bezpečných pracovných postupoch a poskytovať jednoduché, záväzné pravidlá uplatniteľné v každodennej prevádzke bez ohľadu na miesto výkonu práce.

3.5 Zabezpečiť súlad s kontrolou 7.7 prílohy A normy ISO/IEC 27001 a s implementačnými usmerneniami podľa ISO/IEC 27002 pre požiadavky na čistý pracovný stôl a uzamknutú obrazovku.

3.6 Zabezpečiť, aby organizácia vedela preukázať náležitú starostlivosť a pripravenosť na audit bez potreby infraštruktúry na úrovni veľkých podnikov.

4. Roly a zodpovednosti

4.1 Generálny manažér (GM)

4.1.1 Zodpovedá za túto politiku a zabezpečuje, aby bola riadne komunikovaná, pochopená a dodržiavaná všetkými zamestnancami a zmluvnými pracovníkmi.

4.1.2 Zodpovedá za schvaľovanie všetkých výnimiek, riešenie porušení a dohľad nad školeniami súvisiacimi s bezpečnými pracovnými postupmi.

4.1.3 Musí vykonávať alebo delegovať pravidelné kontroly (najmenej štvrťročne) na potvrdenie, že fyzické a digitálne pracoviská spĺňajú požiadavky tejto politiky.

4.2 Určený pracovník (ak je pridelený)

4.2.1 Môže mu byť pridelená zodpovednosť za implementáciu technických nastavení (napr. nastavenia časového limitu uzamknutia obrazovky) alebo za distribúciu fyzických úložných prostriedkov (napr. uzamykateľné zásuvky).

4.2.2 Podporuje GM tým, že nahlasuje nesúlad, zabezpečuje bezpečnostné pripomienky týkajúce sa pracoviska a sleduje nápravné opatrenia pri identifikovaných problémoch.

4.2.3 Pomáha zabezpečiť, aby všetci zamestnanci mali tam, kde je to možné, prístup k vhodným uzamykacím mechanizmom alebo bezpečným úložným priestorom.

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Požiadavky na preskúmanie a aktualizáciu

9.1 GM musí túto politiku preskúmať najmenej raz ročne a po ktorejkoľvek z nasledujúcich udalostí:

9.1.1 zavedenie nových kancelárskych priestorov, zariadení alebo zdieľaných systémov,

9.1.2 zmeny uplatniteľných právnych alebo certifikačných požiadaviek,

9.1.3 zistenia z auditov, posúdení rizík alebo bezpečnostných incidentov.

9.2 Priebežné aktualizácie musia byť oznámené všetkým zamestnancom e-mailom, pričom sa vyžaduje potvrdenie oboznámenia sa.

9.3 Predchádzajúce verzie tejto politiky musia byť bezpečne uchovávané a overiteľné na účely preukázania priebežného súladu s ISO/IEC 27001 a súvisiacimi rámcami.

10. Súvisiace politiky a nadväznosti

10.1 P2S – Politika rolí a zodpovedností v oblasti správy a riadenia: spresňuje právomoc GM presadzovať pravidlá správania vo fyzickom a digitálnom pracovnom priestore a vykonávať ich audit.

10.2 P4S – Politika riadenia prístupu: podporuje technickú implementáciu uzamknutia obrazovky a bezpečných postupov prihlasovania do pracovných staníc.

10.3 P8S – Politika povedomia a školenia o informačnej bezpečnosti: posilňuje školenie správania potrebné na súlad s politikou.

10.4 P17S – Politika ochrany údajov a súkromia: definuje povinnosti pri nakladaní s osobnými a citlivými údajmi a ich ochrane v súlade s GDPR.

10.5 P30S – Politika reakcie na incidenty: poskytuje rámec eskalácie a reakcie, ak porušenie vedie k odkrytiu údajov alebo k porušeniu ochrany osobných údajov.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 7.2: vyžaduje, aby si všetci pracovníci boli vedomí bezpečnostných zodpovedností vrátane fyzickej ochrany.

11.1.2 Kapitola 8.1: prevádzkové kontroly musia zabezpečiť primerané fyzické a logické ochranné opatrenia.

11.2 ISO/IEC 27002

11.2.1 Kontrola 7.7: poskytuje podrobné usmernenia na zavedenie, komunikáciu a presadzovanie požiadaviek na čistý pracovný stôl a uzamknutú obrazovku.

11.3 NIST SP 800-53 Rev.5

11.3.1 PE-2: stanovuje požiadavky na riadenie fyzického prístupu vrátane správania pracovníkov v zabezpečených prostrediach.

11.3.2 AC-11: vyžaduje funkciu uzamknutia relácie pracovných staníc na zabránenie neoprávnenému zobrazeniu alebo interakcii.

11.4 Nariadenie EÚ GDPR

11.4.1 Článok 32: vyžaduje, aby organizácie chránili osobné údaje pomocou fyzických a technických ochranných opatrení vrátane pracovných staníc a dokumentov.

11.5 Smernica EÚ NIS2

11.5.1 Článok 21(2)(d): vyžaduje, aby organizácie zaviedli politiky fyzického a logického prístupu založené na riziku.

11.6 Nariadenie EÚ DORA

11.6.1 Článok 9(2)(f): vyžaduje politiky bezpečnosti IKT vrátane bezpečnej hygieny pracoviska pre subjekty finančného sektora a ich dodávateľské reťazce.

11.7 COBIT 2019

11.7.1 DSS01.06: vyžaduje postupy ochrany aktív vrátane fyzických bezpečnostných opatrení na pracoviskách a médiách.

11.7.2 DSS05.02: podporuje uplatňovanie bezpečnostných postupov koncových používateľov v rôznych prevádzkových prostrediach.