					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P10S					Název dokumentu: **Politika čistého stolu a obrazovky**							
Verze: 1.0		Datum účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Standard		Postup		Formulář		Registr		Jiné	

Historie revizí				
Číslo revize	**Datum revize**	**Změny**	**Přezkoumal**	**Vlastník procesu**

Schválení			
Jméno	**Funkce**	**Datum**	**Podpis**

Soulad s normami a právními předpisy

Norma/právní předpis	Ustanovení/článek	Komentář
ISO/IEC 27001:2022	Články 7.2, 8	
ISO/IEC 27002:2022	Opatření 7	
NIST SP 800-53 Rev.5	PE-2, AC-11	
směrnice EU NIS2	Článek 21 odst. 2 písm. d)	
nařízení EU DORA	Článek 9 odst. 2 písm. f)	
COBIT 2019	DSS01.06, DSS05	
GDPR EU	Článek 32	

1. Účel

1.1 Tato politika stanoví závazná pravidla pro udržování bezpečného pracovního prostředí tím, že zajišťuje, aby na stolech, pracovních stanicích a zobrazovacích zařízeních nezůstávaly v době nepřítomnosti uživatele viditelně přístupné důvěrné informace.

1.2 Jejím hlavním účelem je zabránit neoprávněnému přístupu k citlivým informacím prostřednictvím ponechaných výtisků bez dozoru, neuzamčených obrazovek nebo nesprávně uložených vyměnitelných médií, a to jak v kancelářském prostředí, tak při práci na dálku.

1.3 Postupy čistého stolu a čisté obrazovky vymezené v této politice posilují schopnost organizace splnit požadavky certifikace ISO/IEC 27001 tím, že minimalizují zbytečná rizika zpřístupnění informací. Tyto postupy zároveň poskytují zákazníkům, partnerům a auditorům ujištění, že informační bezpečnost bereme vážně i v prostředích s omezenými zdroji.

1.4 Tato politika podporuje kulturu odpovědnosti a bezpečnostního povědomí a zajišťuje, aby veškerý personál bez ohledu na roli nebo technickou odbornost rozuměl své odpovědnosti za ochranu informací společnosti a zákazníků před vizuálním zpřístupněním, odcizením nebo ztrátou.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 všechny zaměstnance, smluvní pracovníky, stážisty a dočasné pracovníky používající pracovní stanice, pracovní stoly nebo mobilní zařízení ve vlastnictví společnosti nebo jim osobně přidělené,

2.1.2 všechna fyzická místa využívaná k obchodní činnosti, včetně vyhrazených kanceláří, sdílených kancelářských prostor a vzdálených/domácích pracovišť,

2.1.3 všechna digitální zařízení se zobrazovací funkcí, včetně stolních počítačů, notebooků, tabletů a externích monitorů používaných pro obchodní účely.

2.2 Tato politika se vztahuje také na veškerá fyzická nebo digitální aktiva, která mohou zobrazovat, obsahovat nebo přenášet citlivé informace, včetně:

2.2.1 tištěných záznamů nebo ručně psaných poznámek,

2.2.2 USB disků, CD a externích pevných disků,

2.2.3 mobilních telefonů používaných pro pracovní zprávy nebo e-mail,

2.2.4 počítačových monitorů a projektorů připojených k pracovním systémům.

2.3 Tato politika se uplatňuje i mimo běžnou pracovní dobu a při nestandardních činnostech (např. údržba mimo pracovní dobu nebo práce v rámci reakce na mimořádnou událost).

3. Cíle

3.1 Prosazovat praktická a konzistentní opatření, která zajistí, že na stolech, obrazovkách ani ve sdílených prostorech nezůstanou bez ochrany žádné citlivé informace.

3.2 Minimalizovat riziko neoprávněného přístupu jak z interních zdrojů (např. neúmyslný přístup jiných zaměstnanců), tak z externích hrozeb (např. návštěvníci, úklidový personál nebo dodavatelé).

3.3 Podpořit omezení fyzického a logického přístupu tím, že zaměstnanci budou povinni aktivně zabezpečit pracovní materiály a při opuštění pracoviště uzamknout počítače.

3.4 Posilovat povědomí zaměstnanců o bezpečných pracovních postupech a poskytovat jednoduchá, vymahatelná pravidla použitelná při každodenní činnosti bez ohledu na místo výkonu práce.

3.5 Zajistit soulad s přílohou A normy ISO/IEC 27001, opatřením 7.7, a s implementačními pokyny dle ISO/IEC 27002 pro požadavky na čistý stůl a čistou obrazovku.

3.6 Zajistit, aby organizace mohla doložit náležitou péči a připravenost na audit bez potřeby enterprise infrastruktury.

4. Role a odpovědnosti

4.1 generální ředitel (GM)

4.1.1 Je vlastníkem této politiky a zajišťuje, aby byla řádně komunikována, pochopena a dodržována všemi zaměstnanci a smluvními pracovníky.

4.1.2 Odpovídá za schvalování všech výjimek, řešení porušení a dohled nad školením souvisejícím s bezpečnými pracovními postupy.

4.1.3 Musí provádět nebo delegovat pravidelné kontroly (nejméně čtvrtletně) za účelem ověření, že fyzické i digitální pracovní prostory splňují požadavky této politiky.

4.2 pověřený pracovník (je-li určen)

4.2.1 Může mu být přidělena odpovědnost za implementaci technických nastavení (např. nastavení časového limitu obrazovky) nebo za distribuci prostředků pro fyzické ukládání (např. uzamykatelné zásuvky).

4.2.2 Podporuje GM tím, že hlásí případy nesouladu, zajišťuje připomínky k bezpečnosti pracovního prostoru a sleduje nápravná opatření při zjištění problémů.

4.2.3 Pomáhá zajistit, aby všichni zaměstnanci měli v rámci možností přístup k vhodným uzamykacím mechanismům nebo zabezpečeným úložným prostorám.

[... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ...]

9. Požadavky na přezkoumávání a aktualizaci

9.1 GM musí tuto politiku přezkoumat nejméně jednou ročně a po kterékoli z následujících událostí:

9.1.1 zavedení nových kancelářských prostor, zařízení nebo sdílených systémů,

9.1.2 změny příslušných právních požadavků nebo certifikačních požadavků,

9.1.3 zjištění z auditů, hodnocení rizik nebo bezpečnostních incidentů.

9.2 Průběžné aktualizace musí být oznámeny všem zaměstnancům e-mailem, přičemž je vyžadováno potvrzení seznámení.

9.3 Předchozí verze této politiky musí být bezpečně uchovávány a auditovatelné, aby bylo možné doložit průběžný soulad s ISO/IEC 27001 a souvisejícími rámci.

10. Související politiky a vazby

10.1 P2S – Politika rolí a odpovědností v oblasti správy a řízení: upřesňuje pravomoc GM prosazovat a auditovat chování ve fyzických a digitálních pracovních prostorech.

10.2 P4S – Politika řízení přístupu: podporuje technickou implementaci uzamykání obrazovky a bezpečných postupů přihlašování k pracovní stanici.

10.3 P8S – Politika bezpečnostního povědomí a školení: posiluje behaviorální školení potřebné pro dodržování této politiky.

10.4 P17S – Politika ochrany dat a soukromí: stanoví povinnosti při nakládání s osobními a citlivými údaji a jejich ochraně v souladu s GDPR.

10.5 P30S – Politika reakce na incidenty: poskytuje rámec pro eskalaci a reakci v případech, kdy porušení povede ke zpřístupnění dat nebo k bezpečnostnímu incidentu.

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Článek 7.2: Vyžaduje, aby si veškerý personál byl vědom bezpečnostních odpovědností, včetně fyzické ochrany.

11.1.2 Článek 8.1: Provozní opatření musí zajistit odpovídající fyzickou a logickou ochranu.

11.2 ISO/IEC 27002

11.2.1 Opatření 7.7: Poskytuje podrobný návod pro stanovení, komunikaci a prosazování požadavků na čistý stůl a čistou obrazovku.

11.3 NIST SP 800-53 Rev.5

11.3.1 PE-2: Stanoví očekávání v oblasti řízení fyzického přístupu, včetně chování personálu v zabezpečeném prostředí.

11.3.2 AC-11: Vyžaduje funkci uzamčení relace na pracovních stanicích, aby se zabránilo neoprávněnému zobrazení nebo interakci.

11.4 GDPR EU

11.4.1 Článek 32: Vyžaduje, aby organizace chránily osobní údaje pomocí fyzických a technických bezpečnostních opatření, včetně ochrany pracovních stanic a dokumentů.

11.5 směrnice NIS2

11.5.1 Článek 21 odst. 2 písm. d): Vyžaduje, aby organizace zavedly politiky fyzického a logického přístupu založené na rizicích.

11.6 nařízení DORA

11.6.1 Článek 9 odst. 2 písm. f): Vyžaduje politiky bezpečnosti ICT, včetně bezpečné hygieny pracovního prostoru, pro subjekty finančního sektoru a jejich dodavatelské řetězce.

11.7 COBIT 2019

11.7.1 DSS01.06: Vyžaduje postupy ochrany aktiv, včetně fyzických bezpečnostních opatření pro pracovní prostory a média.

11.7.2 DSS05.02: Podporuje prosazování bezpečnostních postupů koncových uživatelů napříč provozními prostředími.