					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P10					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	Článok 6.1.3, článok 8	plán ošetrenia rizík, prevádzkové plánovanie a riadenie a opatrenia pre zabezpečené pracoviská
ISO/IEC 27002:2022	Opatrenie 7	opatrenia zamerané na správanie a prostredie na ochranu fyzických informácií ponechaných bez dozoru
NIST SP 800-53 Rev.5	PE-2, PS-7, MP-6, AC-11, CM-6, IA-5	fyzický prístup, bezpečnosť externého personálu, likvidácia médií, uzamknutie relácie, riadenie konfigurácie a autentifikačných prostriedkov
GDPR EÚ	Článok 5 ods. 1 písm. f), 32; odôvodnenie 39	integrita údajov, dôvernosť a fyzické ochranné opatrenia pre údaje
Smernica EÚ NIS2	Článok 21 ods. 2 písm. d), 21 ods. 3	politiky fyzickej bezpečnosti, správania používateľov a prevencie úniku údajov
Nariadenie EÚ DORA	Články 5, 8, 9	interné riadenie a správa, IKT a riadenie incidentov vrátane fyzickej bezpečnosti
COBIT 2019	DSS01, DSS05, MEA	riadené prevádzkové činnosti, bezpečnostné služby a monitorovanie súladu

1. Účel

1.1 Táto politika stanovuje povinné opatrenia na ochranu citlivých informácií tým, že vyžaduje bezpečné nakladanie s fyzickými dokumentmi, pracovnými stanicami, obrazovkami a vymeniteľnými médiami v kancelárskom prostredí aj na zdieľaných pracoviskách.

1.2 Podporuje opatrenie 7.7 prílohy A normy ISO/IEC 27001 tým, že zavádza behaviorálne opatrenia a technické postupy na zmiernenie rizika neoprávneného sprístupnenia, odcudzenia alebo straty údajov v dôsledku informácií ponechaných bez dozoru alebo viditeľne vystavených.

1.3 Táto politika posilňuje fyzickú a informačnú bezpečnosť v každodennej prevádzke a podporuje súlad s uplatniteľnými zákonnými, zmluvnými a regulačnými povinnosťami.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky osoby pôsobiace vo fyzických pracovných priestoroch alebo do nich vstupujúce, vrátane:

2.1.1 zamestnancov na dobu neurčitú aj určitú

2.1.2 zmluvných pracovníkov, konzultantov, dodávateľov a stážistov

2.1.3 poskytovateľov služieb tretích strán a návštev pracoviska s prístupom k citlivým informáciám

2.2 Požiadavky sa uplatňujú v:

2.2.1 samostatných kanceláriách, boxoch a otvorených kancelárskych priestoroch

2.2.2 zasadacích miestnostiach a zdieľaných priestoroch na spoluprácu

2.2.3 priestoroch s tlačiarňami, na recepčných pultoch a v kopírovacích miestnostiach

2.2.4 priestoroch, kde sa používajú vzdialené pracovné stanice alebo zdieľané kiosky

2.3 Táto politika sa vzťahuje aj na dočasné alebo hybridné pracovné prostredia (napr. hot-desking) a na verejne prístupné prostredia, v ktorých existuje riziko odpozorovania obrazovky alebo údajov ponechaných bez dozoru.

3. Ciele

3.1 Predchádzať neoprávnenému prístupu k dôverným, citlivým alebo regulovaným informáciám ponechaným vo fyzickej alebo digitálnej podobe bez ochrany.

3.2 Presadzovať jednotný bezpečnostný štandard vo všetkých pracovných prostrediach prostredníctvom fyzických bezpečnostných opatrení, konfigurácie pracovných staníc a správania koncových používateľov.

3.3 Znižovať riziko porušenia ochrany súkromia, straty duševného vlastníctva a úniku údajov spôsobených nedbanlivosťou alebo opomenutím.

3.4 Začleniť zásady čistého pracovného stola a uzamknutej obrazovky do kultúry organizácie, a tým podporiť prevádzkovú disciplínu, auditovateľnosť a obhájiteľnosť vo vzťahu k regulačným požiadavkám.

3.5 Podporovať súlad s ISO/IEC 27001, článkom 32 GDPR EÚ, článkom 15 smernice EÚ NIS2 a ďalšími požiadavkami fyzickej bezpečnosti vzťahujúcimi sa na kritické údaje alebo osobné údaje.

4. Roly a zodpovednosti

4.1 vrcholový manažment

4.1.1 Schvaľuje túto politiku a podporuje kultúru bezpečnostného povedomia vo všetkých organizačných jednotkách.

4.1.2 Prideľuje primerané zdroje na uplatňovanie politiky, kampane na zvyšovanie povedomia a mechanizmy fyzických kontrol.

4.2 CISO / manažér ISMS

4.2.1 Je vlastníkom tejto politiky a zabezpečuje jej súlad s ISO/IEC 27001:2022, požiadavkami auditu a stratégiami ošetrenia rizík.

4.2.2 Vypracúva programy zvyšovania povedomia a kontrolné mechanizmy s cieľom zabezpečiť jednotné zavedenie naprieč pracoviskami a v podmienkach hybridného režimu práce.

4.2.3 Koordinuje činnosti so správou zariadení a majetku a s IT s cieľom zabezpečiť zavedenie primeraných fyzických bezpečnostných opatrení.

[... 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 Harmonogram preskúmania politiky

9.1.1 Táto politika sa musí preskúmať:

9.1.1.1 najmenej raz ročne

9.1.1.2 po každej nezhode z auditu súvisiacej s vystavením pracoviska alebo obrazovky

9.1.1.3 po fyzickom alebo environmentálnom incidente (napr. krádež zariadenia, neoprávnené nasledovanie oprávnenej osoby pri vstupe, sledovanie)

9.1.1.4 pri zavedení nových usporiadaní kancelárií, politík pracovísk alebo modelov pracoviska (napr. hot-desking, vzdialené pracovné huby)

9.2 Zodpovední vlastníci

9.2.1 Vlastníkom politiky je CISO alebo určený manažér ISMS.

9.2.2 Proces preskúmania musí zahŕňať:

9.2.2.1 tímy správy zariadení a podnikovej bezpečnosti

9.2.2.2 IT a infraštruktúru na uplatňovanie opatrení súvisiacich so zariadeniami

9.2.2.3 oddelenie ľudských zdrojov a právne oddelenie na uplatňovanie pravidiel správania a zosúladenie disciplinárnych postupov

9.2.3 Všetky aktualizácie politiky musia podliehať riadeniu verzií, byť schválené riadiacim výborom pre ISMS a opätovne distribuované spolu s novým potvrdením oboznámenia sa, ak sa to vyžaduje.

9.3 Oznámenie zmien

9.3.1 Používatelia musia byť o významných aktualizáciách informovaní prostredníctvom:

9.3.1.1 intranetového centra politík alebo portálu

9.3.1.2 cielených e-mailových oznámení

9.3.1.3 opakovaných vstupných poučení a štvrťročných briefingov

9.3.1.4 povinných výziev na potvrdenie oboznámenia sa pri každom novom kritickom ustanovení o uplatňovaní pravidiel

10. Súvisiace politiky a väzby

10.1 Táto politika je zosúladená s nasledujúcimi dokumentmi a podporuje ich:

10.1.1 P1 – Politika informačnej bezpečnosti: stanovuje očakávania týkajúce sa správania používateľov a fyzickej bezpečnosti, ktoré tvoria základ tejto politiky.

10.1.2 P3 – Politika prijateľného používania: upravuje zodpovednosť používateľov za ochranu údajov a systémov vrátane fyzického prostredia.

10.1.3 P6 – Politika riadenia rizík: zahŕňa riziká fyzických pracovísk ako súčasť celopodnikovej analýzy informačných rizík.

10.1.4 P12 – Politika správy aktív: podporuje sledovanie a bezpečné nakladanie so zariadeniami a médiami ponechanými na pracovných stoloch.

10.1.5 P13 – Politika klasifikácie a označovania údajov: vytvára väzbu na uplatňovanie zásad čistého pracovného stola pri fyzických dokumentoch označených ako dôverné alebo na interné použitie.

10.1.6 P14 – Politika uchovávania a likvidácie údajov: usmerňuje uchovávanie fyzických dokumentov, skartáciu a postupy nakladania s nádobami na likvidáciu.

10.1.7 P22 – Politika logovania a monitorovania: môže sa použiť na monitorovanie stavu uzamknutia pracovnej stanice, doby nečinnosti alebo kamerových záznamov pracoviska tam, kde je to prípustné.

10.2 Tieto súvisiace politiky vytvárajú integrovanú bezpečnostnú kultúru, ktorá spája povedomie používateľov, fyzické bezpečnostné opatrenia a zodpovednosť za konanie s cieľom zabezpečiť odolné pracoviská.

11. Referenčné normy a rámce

11.1 Táto politika je zosúladená s medzinárodne uznávanými normami a právnymi požiadavkami, ktoré vyžadujú ochranu citlivých informácií vo fyzickom prostredí a prostredníctvom správania používateľov.

11.2 ISO/IEC 27001

11.2.1 Článok 6.1.3 – plán ošetrenia rizík: podporuje zavedenie opatrení na zmiernenie fyzických a environmentálnych rizík vrátane rizík spojených so správaním používateľov v otvorených pracovných priestoroch.

11.2.2 Článok 8.1 – prevádzkové plánovanie a riadenie: stanovuje prevádzkové ochranné opatrenia na riadenie zabezpečených pracovísk a používania zariadení.

11.3 ISO/IEC 27002:2022 – Opatrenie 7

11.3.1 Toto opatrenie vyžaduje behaviorálne opatrenia a ochranu prostredia na predchádzanie neoprávnenému prístupu k informáciám prostredníctvom médií, obrazoviek alebo tlačených materiálov ponechaných bez dozoru. Táto politika zavádza hygienu fyzického pracoviska, používanie uzamknutia obrazovky a likvidáciu citlivých dokumentov.

11.4 NIST SP 800-53 Rev.5

11.4.1 PE-2 (oprávnenia fyzického prístupu): väzba prostredníctvom obmedzení pracovísk a uplatňovania uzamknutého úložiska vo vysokorizikových prostrediach.

11.4.2 PS-7 (bezpečnosť externého personálu): uplatňuje sa prostredníctvom požiadaviek na čistý pracovný stôl a uzamknutú obrazovku rozšírených na zmluvných pracovníkov a používateľov tretích strán.

11.4.3 MP-6 (sanitizácia médií) a AC-11 (uzamknutie relácie): implementované prostredníctvom postupov bezpečnej likvidácie a povinných časovačov uzamknutia obrazovky.

11.4.4 CM-6 (nastavenia konfigurácie) a IA-5 (riadenie autentifikátorov): podporujú technické uplatňovanie uzamknutia obrazovky a riadenia relácií na koncových zariadeniach.

11.5 GDPR EÚ (2016/679)

11.5.1 Článok 5 ods. 1 písm. f): vyžaduje integritu a dôvernosť osobných údajov vrátane ochrany pred fyzickým vystavením alebo zobrazením neoprávneným osobám.

11.5.2 Článok 32 – bezpečnosť spracúvania: vyžaduje primerané fyzické a organizačné opatrenia na ochranu osobných údajov pred náhodným alebo nezákonným zničením, stratou alebo neoprávneným sprístupnením, čo sa dosahuje prostredníctvom kontrol pracovného stola a obrazovky.

11.5.3 Odôvodnenie 39: vyžaduje obmedzenie prístupu k osobným údajom na oprávnené osoby; to zahŕňa aj ich zabezpečenie vo fyzickej forme, ak sú ponechané bez dozoru.

11.6 Smernica EÚ NIS2 (2022/2555)

11.6.1 Článok 21 ods. 2 písm. d): vyžaduje politiky a postupy týkajúce sa fyzickej bezpečnosti a bezpečnosti prostredia vrátane ochrany informácií na úrovni pracoviska.

11.6.2 Článok 21 ods. 3: podporuje bezpečnostnú kultúru, ktorá zahŕňa správne správanie používateľov, povedomie a predchádzanie neúmyselným únikom údajov; táto politika to podporuje prostredníctvom behaviorálnych opatrení.

11.7 Nariadenie EÚ DORA (2022/2554)

11.7.1 Článok 5 – interné riadenie, správa a kontrola: vyžaduje, aby všetky riziká súvisiace s IKT vrátane ľudských a environmentálnych hrozieb boli riadené prostredníctvom vynútiteľných politík.

11.7.2 Článok 8 – riadenie rizík IKT: vyžaduje ochranné opatrenia v digitálnom aj fyzickom kontexte, aby používatelia pracujúci na diaľku, na pobočkách a vo vlastných priestoroch nevytvárali neriadenú expozíciu.

11.7.3 Článok 9 – riadenie incidentov: vyžaduje, aby environmentálne alebo behaviorálne zlyhania vedúce k vystaveniu údajov boli zaznamenané v záznamoch, klasifikované a riešené primeranými nápravnými opatreniami.

11.8 COBIT 2019

11.8.1 DSS01 – riadené prevádzkové činnosti: zabezpečuje prevádzkovú disciplínu pri ochrane fyzických pracovísk a systémov prostredníctvom opakovateľných opatrení.

11.8.2 DSS05 – riadené bezpečnostné služby: podporuje ochranu údajov, zariadení a koncových bodov prístupu prostredníctvom uplatňovania pravidiel správania, ako sú zásady čistého pracovného stola.

11.8.3 MEA03 – monitorovanie, hodnotenie a posudzovanie súladu: podporuje auditovanie fyzických bezpečnostných opatrení a zavedenia politiky v každodennej praxi organizácie.