					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P10					Název dokumentu: **Politika čistého stolu a uzamčené 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**

V souladu s normami a právními předpisy

Norma/právní předpis	Článek/ustanovení	Komentář
ISO/IEC 27001:2022	Článek 6.1.3, článek 8	Plán ošetření rizik, operativní plánování a řízení zabezpečených pracovních prostor
ISO/IEC 27002:2022	Opatření 7	Behaviorální a environmentální opatření k zabezpečení fyzických informací ponechaných bez dozoru
NIST SP 800-53 Rev.5	PE-2, PS-7, MP-6, AC-11, CM-6, IA-5	Fyzický přístup, bezpečnost externích pracovníků, likvidace médií, uzamčení relace, nastavení konfigurace a správa autentizačních prostředků
GDPR EU	Články 5 odst. 1 písm. f), 32; bod odůvodnění 39	Integrita dat, důvěrnost a fyzická bezpečnostní opatření pro ochranu dat
směrnice NIS2 EU	Články 21 odst. 2 písm. d), 21 odst. 3	Politiky fyzické bezpečnosti, chování uživatelů a prevence úniku dat
nařízení DORA EU	Články 5, 8, 9	Vnitřní správa a řízení, ICT a řízení incidentů zahrnující fyzickou bezpečnost
COBIT 2019	DSS01, DSS05, MEA	Řízený provoz, bezpečnostní služby a monitorování souladu

1. Účel

1.1 Tato politika stanoví povinná opatření k ochraně citlivých informací tím, že vyžaduje bezpečné nakládání s fyzickými dokumenty, pracovními stanicemi, obrazovkami a vyměnitelnými médii v kancelářském prostředí i ve sdílených pracovních prostorech.

1.2 Podporuje přílohu A normy ISO/IEC 27001, opatření 7.7, prosazováním behaviorálních a technických postupů zmírňujících riziko neoprávněného zpřístupnění, odcizení nebo ztráty dat v důsledku ponechání informací bez dozoru nebo jejich viditelnosti.

1.3 Tato politika posiluje fyzickou bezpečnost a bezpečnost informací v každodenním provozu a podporuje soulad s příslušnými právními, smluvními a regulatorními požadavky.

2. Rozsah

2.1 Tato politika se vztahuje na veškerý personál, který pracuje ve fyzických pracovních prostorech nebo do nich vstupuje, včetně:

2.1.1 zaměstnanců na dobu neurčitou i určitou

2.1.2 dodavatelů, konzultantů, obchodních partnerů a stážistů

2.1.3 poskytovatelů služeb třetích stran a návštěvníků pracoviště s přístupem k citlivým informacím

2.2 Požadavky se uplatňují v:

2.2.1 samostatných kancelářích, kójích a otevřených kancelářských prostorech

2.2.2 zasedacích místnostech a sdílených prostorech pro spolupráci

2.2.3 prostorách s tiskárnami, na recepcích a v kopírovacích místnostech

2.2.4 místech, kde se používají vzdálené pracovní stanice nebo sdílené kiosky

2.3 Tato politika se rovněž vztahuje na dočasná nebo hybridní pracovní prostředí (např. hot desking) a veřejně přístupná prostředí, kde existuje riziko vizuálního odpozorování údajů nebo ponechání dat bez dozoru.

3. Cíle

3.1 Předcházet neoprávněnému přístupu k důvěrným, citlivým nebo regulovaným informacím ponechaným v nezakryté fyzické nebo digitální podobě.

3.2 Podporovat standardizovanou úroveň bezpečnosti napříč všemi pracovními prostředími prostřednictvím fyzických bezpečnostních opatření, konfigurace pracovních stanic a chování koncových uživatelů.

3.3 Snižovat riziko narušení ochrany soukromí, ztráty duševního vlastnictví a exfiltrace dat způsobené nedbalostí nebo opomenutím.

3.4 Začlenit zásady čistého stolu a uzamčené obrazovky do kultury organizace a tím podpořit provozní disciplínu, auditovatelnost a schopnost právně doložit správný postup.

3.5 Podporovat soulad s ISO/IEC 27001, článkem 32 GDPR, článkem 21 NIS2 a dalšími požadavky na fyzickou bezpečnost vztahujícími se na kritická data nebo osobní údaje.

4. Role a odpovědnosti

4.1 Vrcholové vedení

4.1.1 Schvaluje tuto politiku a podporuje kulturu bezpečnostního povědomí napříč všemi organizačními útvary.

4.1.2 Přiděluje odpovídající zdroje pro uplatňování této politiky, kampaně na podporu povědomí a mechanismy fyzických kontrol.

4.2 Ředitel informační bezpečnosti (CISO) / manažer ISMS

4.2.1 Je vlastníkem této politiky a zajišťuje její soulad s ISO/IEC 27001:2022, požadavky auditu a strategiemi ošetření rizik.

4.2.2 Vytváří programy povědomí a opatření k zajištění jednotné implementace napříč pracovišti a v hybridním pracovním režimu.

4.2.3 Koordinuje činnosti se správou budov a majetku a IT za účelem zajištění odpovídajících fyzických bezpečnostních opatření.

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

9. Požadavky na přezkoumávání a aktualizaci

9.1 Harmonogram přezkumu politiky

9.1.1 Tato politika musí být přezkoumána:

9.1.1.1 nejméně jednou ročně

9.1.1.2 po jakékoli neshodě z auditu související s expozicí pracovního prostoru nebo obrazovky

9.1.1.3 po fyzickém nebo environmentálním incidentu (např. krádež zařízení, neoprávněný vstup v závěsu za oprávněnou osobou, vizuální odpozorování)

9.1.1.4 při zavedení nového uspořádání kanceláří, pravidel pracoviště nebo modelů pracovních prostor (např. hot desking, vzdálená centra)

9.2 Odpovědní vlastníci

9.2.1 Vlastníkem politiky je ředitel informační bezpečnosti (CISO) nebo jmenovaný manažer ISMS.

9.2.2 Do procesu přezkumu musí být zapojeni:

9.2.2.1 týmy správy budov a podnikové bezpečnosti

9.2.2.2 IT a infrastruktura pro vynucování opatření souvisejících se zařízeními

9.2.2.3 HR a právní a compliance pro prosazování požadovaného chování a sladění disciplinárních postupů

9.2.3 Všechny aktualizace politiky musí být vedeny v režimu správy verzí, schváleny Řídicím výborem pro bezpečnost informací a znovu distribuovány s opětovným potvrzením seznámení, pokud je to vyžadováno.

9.3 Komunikace změn

9.3.1 Uživatelé musí být o podstatných aktualizacích informováni prostřednictvím:

9.3.1.1 intranetového centra politik nebo portálu

9.3.1.2 cílené e-mailové komunikace

9.3.1.3 opakovacích školení při nástupu a čtvrtletních briefingů

9.3.1.4 povinných výzev k potvrzení seznámení u všech nových kritických ustanovení o vynucování

10. Související politiky a vazby

10.1 Tato politika je v souladu s následujícími politikami a podporuje je:

10.1.1 P1 – P01 Politika informační bezpečnosti: Stanoví očekávání týkající se chování uživatelů a fyzické bezpečnosti, která jsou základem této politiky.

10.1.2 P3 – Zásady přípustného užívání: Upravují odpovědnost uživatelů za ochranu dat a systémů, včetně fyzického prostředí.

10.1.3 P6 – Politika řízení rizik: Zahrnuje rizika fyzických pracovních prostor jako součást celopodnikové analýzy informačních rizik.

10.1.4 P12 – Politika správy aktiv: Podporuje evidenci a bezpečné nakládání se zařízeními a médii ponechanými na stolech.

10.1.5 P13 – Politika klasifikace dat a označování: Navazuje na prosazování zásad čistého stolu u fyzických dokumentů označených jako důvěrné nebo pro interní použití.

10.1.6 P14 – Politika uchovávání údajů a likvidace: Stanoví pravidla pro uchovávání fyzických dokumentů, skartaci a nakládání s určenými nádobami.

10.1.7 P22 – Politika protokolování a monitorování: Může být použita k monitorování stavu uzamčení pracovních stanic, doby nečinnosti nebo kamerových záznamů pracovních prostor, je-li to povoleno.

10.2 Tyto související politiky vytvářejí integrovanou bezpečnostní kulturu kombinující povědomí uživatelů, fyzická bezpečnostní opatření a odpovědnost za účelem zajištění odolných pracovních prostor.

11. Referenční normy a rámce

11.1 Tato politika je v souladu s mezinárodně uznávanými normami a právními požadavky, které vyžadují ochranu citlivých informací ve fyzickém prostředí a prostřednictvím chování uživatelů.

11.2 ISO/IEC 27001

11.2.1 Článek 6.1.3 – Plán ošetření rizik: Podporuje implementaci opatření ke zmírnění fyzických a environmentálních rizik, včetně rizik spojených s chováním uživatelů v otevřených pracovních prostorech.

11.2.2 Článek 8.1 – Operativní plánování a řízení: Stanoví provozní bezpečnostní opatření pro správu zabezpečených pracovních prostor a používání zařízení.

11.3 ISO/IEC 27002:2022 – Opatření 7

11.3.1 Toto opatření vyžaduje behaviorální a environmentální ochranu, aby se zabránilo neoprávněnému přístupu k informacím prostřednictvím médií, obrazovek nebo tištěných materiálů ponechaných bez dozoru. Tato politika prosazuje hygienu fyzického pracovního prostoru, používání uzamčení obrazovky a likvidaci citlivých dokumentů.

11.4 NIST SP 800-53 Rev.5

11.4.1 PE-2 (Physical Access Authorizations): Vazba prostřednictvím omezení pracovních prostor a vynucování uzamčeného ukládání ve vysoce rizikových prostředích.

11.4.2 PS-7 (External Personnel Security): Uplatňuje se prostřednictvím požadavků na čistý stůl a obrazovku rozšířených na dodavatele a uživatele třetích stran.

11.4.3 MP-6 (Media Sanitization) a AC-11 (Session Lock): Implementováno prostřednictvím postupů bezpečné likvidace a povinných časových limitů uzamčení obrazovky.

11.4.4 CM-6 (Configuration Settings) a IA-5 (Authenticator Management): Podporují technické vynucování uzamčení obrazovky a správy relací na koncových zařízeních.

11.5 GDPR EU (2016/679)

11.5.1 Článek 5 odst. 1 písm. f): Prosazuje integritu a důvěrnost osobních údajů, včetně ochrany proti fyzickému vystavení nebo nahlížení neoprávněnými osobami.

11.5.2 Článek 32 – Zabezpečení zpracování: Vyžaduje odpovídající fyzická a organizační opatření k ochraně osobních údajů před náhodným nebo protiprávním zničením, ztrátou nebo neoprávněným zpřístupněním, čehož je dosaženo prostřednictvím opatření pro čistý stůl a uzamčenou obrazovku.

11.5.3 Bod odůvodnění 39: Vyžaduje omezení přístupu k osobním údajům na oprávněné osoby; to zahrnuje i jejich zabezpečení ve fyzické podobě v době nepřítomnosti.

11.6 směrnice NIS2 EU (2022/2555)

11.6.1 Článek 21 odst. 2 písm. d): Vyžaduje politiky a postupy týkající se fyzické a environmentální bezpečnosti, včetně ochrany informací na úrovni pracoviště.

11.6.2 Článek 21 odst. 3: Podporuje bezpečnostní kulturu zahrnující správné chování uživatelů, povědomí a prevenci neúmyslných úniků dat, což je podporováno behaviorálními opatřeními této politiky.

11.7 nařízení DORA EU (2022/2554)

11.7.1 Článek 5 – Vnitřní správa a řízení a kontrola: Vyžaduje, aby všechna rizika související s ICT, včetně lidských a environmentálních hrozeb, byla řízena prostřednictvím vymahatelných politik.

11.7.2 Článek 8 – Řízení rizik v oblasti ICT: Prosazuje bezpečnostní opatření v digitálním i fyzickém kontextu a zajišťuje, aby uživatelé pracující na dálku, na pobočkách a v on-premise prostředí nevytvářeli neřízenou expozici.

11.7.3 Článek 9 – Řízení incidentů: Vyžaduje, aby environmentální nebo behaviorální pochybení vedoucí k expozici dat byla protokolována, klasifikována a řešena odpovídajícími nápravnými opatřeními.

11.8 COBIT 2019

11.8.1 DSS01 – Managed Operations: Zajišťuje provozní disciplínu při ochraně fyzických pracovních prostor a systémů prostřednictvím opakovatelných opatření.

11.8.2 DSS05 – Managed Security Services: Podporuje ochranu dat, zařízení a přístupových koncových bodů prostřednictvím behaviorálního prosazování, jako jsou zásady čistého stolu.

11.8.3 MEA03 – Monitor, Evaluate, and Assess Compliance: Podporuje audit fyzických bezpečnostních opatření a uplatňování politiky v každodenní podnikové praxi.