					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P09S					Názov dokumentu: **Politika práce na diaľku**							
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**

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitoly 6.1, 6.2, 8	
ISO/IEC 27002:2022	Kontrola 6	
Smernica EÚ NIS2	Články 21(2)(b), 21(2)(h)	EÚ NIS2
Nariadenie EÚ DORA	Článok 9	EÚ DORA
COBIT 2019	DSS05, APO13	COBIT 2019
Nariadenie EÚ GDPR	Článok 32	EÚ GDPR

1. Účel

1.1 Táto politika stanovuje bezpečnostné požiadavky pre zamestnancov a zmluvných pracovníkov vykonávajúcich prácu na diaľku vrátane práce z domu, zo zdieľaných pracovných priestorov alebo počas cestovania.

1.2 Jej cieľom je chrániť dôvernosť, integritu a dostupnosť informácií organizácie, ku ktorým sa pristupuje mimo prostredí kontrolovaných spoločnosťou.

1.3 Táto politika zabezpečuje súlad s medzinárodnými normami a znižuje riziká, ako sú neoprávnený prístup, strata údajov a prerušenie služieb.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetkých pracovníkov (zamestnancov, zmluvných pracovníkov, konzultantov a dočasných pracovníkov), ktorí pri práci mimo pracoviska pristupujú k systémom, sieťam alebo údajom spoločnosti.

2.2 Zahŕňa:

2.2.1 používanie zariadení pridelených spoločnosťou a súkromných zariadení

2.2.2 prístup prostredníctvom VPN, vzdialenej pracovnej plochy alebo cloudových služieb

2.2.3 bezpečné nakladanie s informáciami mimo priestorov spoločnosti

2.2.4 monitorovanie, ošetrenie výnimiek a uplatňovanie tejto politiky

2.3 Vzťahuje sa na plný aj čiastočný režim práce na diaľku vrátane ad hoc vzdialeného prístupu.

3. Ciele

3.1 Predchádzať neoprávnenému prístupu k systémom spoločnosti alebo citlivým údajom počas práce na diaľku.

3.2 Zabezpečiť, aby zariadenia a komunikačné spojenia používané mimo kancelárie spĺňali základné bezpečnostné požiadavky.

3.3 Udržiavať kontrolu nad oprávneniami vzdialeného prístupu a nad monitorovaním.

3.4 Poskytovať zamestnancom a manažérom jasné usmernenia pre bezpečné postupy práce na diaľku.

3.5 Zabezpečiť súlad s požiadavkami ISO, NIS2, GDPR, DORA a COBIT na vzdialenú a mobilnú prácu.

4. Roly a zodpovednosti

4.1 Generálny manažér (GM)

4.1.1 Schvaľuje režim práce na diaľku a monitoruje dodržiavanie tejto politiky.

4.1.2 Eskaluje bezpečnostné incidenty alebo opakovaný nesúlad.

4.1.3 Preskúmava výnimky a zabezpečuje prijatie následných opatrení po incidente.

4.2 IT podpora alebo externý poskytovateľ IT služieb

4.2.1 Zriaďuje bezpečný vzdialený prístup (napr. VPN, MFA).

4.2.2 Uplatňuje ochranu koncových bodov, šifrovanie a bezpečné konfigurácie zariadení.

4.2.3 Poskytuje používateľom podporu a preveruje technické bezpečnostné problémy.

[... 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 Ročné preskúmanie politiky

9.1.1 Generálny manažér (GM) a IT podpora musia túto politiku preskúmať najmenej raz ročne tak, aby zohľadňovala zmeny v technológiách, pracovnej sile a právnych požiadavkách.

9.2 Spúšťače skoršej aktualizácie

9.2.1 Okamžité preskúmanie sa vyžaduje po:

9.2.1.1 závažnom bezpečnostnom incidente súvisiacom s prácou na diaľku

9.2.1.2 zmenách požiadaviek NIS2, GDPR alebo DORA

9.2.1.3 prechode na novú technológiu vzdialeného prístupu (napr. inú platformu VPN)

9.3 Riadenie verzií a archivácia

9.3.1 Všetky verzie tejto politiky musia byť:

9.3.1.1 datované a schválené generálnym manažérom (GM)

9.3.1.2 označené číslom verzie

9.3.1.3 archivované najmenej tri roky

9.4 Informovanie zamestnancov

9.4.1 Aktualizácie politiky musia byť oznámené všetkým používateľom pracujúcim na diaľku. Pri každej významnej zmene sa vyžaduje potvrdenie oboznámenia sa.

10. Súvisiace politiky a väzby

10.1 Táto politika nadväzuje na tieto dokumenty a podporuje ich:

10.1.1 P2S – Politika rolí a zodpovedností v oblasti správy a riadenia: určuje, kto schvaľuje vzdialený prístup a vykonáva nad ním dohľad

10.1.2 P4S – Politika riadenia prístupu: stanovuje postupy bezpečného zriaďovania a rušenia vzdialeného prístupu

10.1.3 P6S – Politika riadenia rizík: sleduje a vyhodnocuje riziká súvisiace s prístupom mimo pracoviska

10.1.4 P8S – Politika povedomia a školenia o informačnej bezpečnosti: školí používateľov o rizikách práce na diaľku a osvedčených postupoch

10.1.5 P30S – Politika reakcie na incidenty: riadi reakciu na incidenty vzdialeného prístupu, ako sú úniky prihlasovacích údajov alebo strata zariadenia

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 6.1 – plánovanie vzdialeného prístupu na základe rizík

11.1.2 Kapitola 6.2 – upravuje zodpovednosti HR v kontexte mobilnej a vzdialenej práce

11.1.3 Kapitola 8.1 – prevádzkové plánovanie a riadenie vzdialených procesov

11.2 ISO/IEC 27002

11.2.1 Kontrola 6.7 – poskytuje praktické usmernenia k bezpečnosti vzdialenej a mobilnej práce

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-17 – riadenie vzdialeného prístupu, ochrana relácií a bezpečnostné monitorovanie

11.3.2 AC-2 – riadenie účtov pre používateľov mimo pracoviska

11.4 Nariadenie EÚ GDPR

11.4.1 Článok 32 – vyžaduje ochranu údajov „už pri návrhu a štandardne“, a to aj vo vzdialenom prostredí

11.5 Smernica EÚ NIS2

11.5.1 Článok 21(2)(b) – vyžaduje bezpečné používanie sietí a informačných systémov

11.5.2 Článok 21(2)(h) – vyžaduje bezpečnostné opatrenia súvisiace s ľudskými zdrojmi vrátane kontrol mimo pracoviska

11.6 Nariadenie EÚ DORA

11.6.1 Článok 9 – vyžaduje, aby finančné subjekty udržiavali odolnosť IKT vo všetkých prevádzkových režimoch vrátane vzdialeného prístupu

11.7 COBIT 2019

11.7.1 DSS05 – Riadenie bezpečnostných služieb: zahŕňa ochranu koncových bodov a bezpečné postupy práce na diaľku

11.7.2 APO13 – Riadená bezpečnosť: zabezpečuje bezpečné zriaďovanie a dohľad nad rizikami mobilného a vzdialeného prístupu