					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P09					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**

1. Účel

1.1 Táto politika stanovuje záväzné požiadavky na bezpečný výkon práce na diaľku vrátane používania systémov organizácie, prístupu k údajom a vykonávania pracovných povinností mimo priestorov organizácie.

1.2 Zabezpečuje dôvernosť, integritu a dostupnosť informačných aktív, ku ktorým sa pristupuje na diaľku, a ustanovuje kontroly na zmiernenie rizík spojených s distribuovanými pracovnými prostrediami.

1.3 Táto politika napĺňa požiadavky prílohy A, kontroly 6.7 normy ISO/IEC 27001:2022 implementáciou technických a procesných ochranných opatrení prispôsobených podmienkam práce na diaľku.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky osoby oprávnené vykonávať prácu na diaľku vrátane:

2.1.1 zamestnancov (na plný úväzok, čiastočný úväzok alebo na zmluvnom základe)

2.1.2 externých poskytovateľov služieb, konzultantov a dodávateľov

2.1.3 dočasných a projektových pracovníkov so schváleným vzdialeným prístupom

2.2 Politika sa vzťahuje na:

2.2.1 prístup k systémom organizácie prostredníctvom VPN alebo schválených nástrojov vzdialeného prístupu

2.2.2 nakladanie s citlivými a regulovanými informáciami mimo zabezpečených priestorov

2.2.3 používanie zariadení vo vlastníctve organizácie alebo vlastných zariadení používateľa (BYOD)

2.2.4 fyzické bezpečnostné opatrenia a logický prístup v prostrediach práce na diaľku

2.3 Táto politika sa uplatňuje vo všetkých geografických oblastiach a časových pásmach, v ktorých organizácia povoľuje prácu na diaľku, či už pravidelnú, ad hoc, alebo počas udalostí kontinuity činností.

3. Ciele

3.1 Zabezpečiť, aby k interným systémom a informáciám pristupovali na diaľku iba oprávnené osoby.

3.2 Vynucovať používanie šifrovania, viacfaktorovej autentifikácie (MFA) a ochrany koncových bodov na všetkých trasách vzdialeného prístupu.

3.3 Udržiavať primeranú úroveň bezpečnosti voči hrozbám, ako sú phishing, malvér, exfiltrácia údajov a neoprávnené vystavenie systémov.

3.4 Upraviť spôsob prenosu, uchovávania a tlače citlivých údajov v prostrediach mimo pracoviska.

3.5 Zaviesť fyzické bezpečnostné opatrenia, ktoré znižujú viditeľnosť a riziko neoprávneného pozorovania počas vzdialených relácií.

3.6 Zabezpečiť súlad s medzinárodnými regulačnými požiadavkami na vzdialený prístup k údajom vrátane GDPR, NIS2 a DORA.

4. Roly a zodpovednosti

4.1 Vrcholový manažment

4.1.1 Schvaľuje túto politiku a zabezpečuje, aby jej boli pridelené primerané zdroje a aby bola integrovaná do činností HR, IT a bezpečnostných operácií.

4.1.2 Schvaľuje kritériá oprávnenosti na prácu na diaľku a ich uplatnenie pre jednotlivé organizačné jednotky.

4.2 CISO / manažér ISMS

4.2.1 Zodpovedá za túto politiku, udržiava ju a zabezpečuje jej súlad s rizikovým profilom a regulačnými požiadavkami.

4.2.2 Definuje bezpečnostné kontroly pre vzdialený prístup (napr. šifrovanie, ochrana koncových bodov, časové limity relácií).

4.2.3 Schvaľuje spôsob riešenia výnimiek a monitoruje účinnosť kontrol.

[... 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 Frekvencia preskúmania

9.1.1 Táto politika sa musí preskúmavať každoročne alebo častejšie pri:

9.1.1.1 zavedení nových technológií vzdialeného prístupu

9.1.1.2 významnom rozšírení práce na diaľku (napr. iniciatívy hybridnej pracovnej sily)

9.1.1.3 vzniku nových hrozieb, zraniteľností alebo incidentov súvisiacich so vzdialenými prostrediami

9.1.1.4 zmenách relevantných právnych alebo regulačných rámcov

9.2 Vlastníctvo a proces preskúmania

9.2.1 Vlastníkom politiky je CISO. Preskúmanie sa musí koordinovať s:

9.2.1.1 IT prevádzkou a architektúrou

9.2.1.2 HR a správou zariadení (z dôvodu prevádzkových dopadov a dopadov na pracovné priestory)

9.2.1.3 zodpovednou osobou pre ochranu osobných údajov (z dôvodu ochrany súkromia a kontrol cezhraničných prenosov údajov)

9.2.2 Aktualizácie politiky musia byť:

9.2.2.1 schválené Riadiacim výborom ISMS

9.2.2.2 komunikované všetkým dotknutým zamestnancom a zmluvným pracovníkom

9.2.2.3 začlenené do materiálov pre proces nástupu a opakované školenie

9.3 Riadenie dokumentu a distribúcia

9.3.1 Politika musí zahŕňať riadenie verzií, dátum účinnosti a históriu zmien.

9.3.2 Nahradené verzie sa musia uchovávať podľa Politiky správy dokumentov (P14).

9.3.3 Revidované verzie musia vyvolať povinné opätovné potvrdenie oboznámenia sa s politikou pre používateľov oprávnených na prácu na diaľku.

10. Súvisiace politiky a väzby

10.1 Táto politika sa uplatňuje spolu s týmito politikami:

10.1.1 P1 – Politika informačnej bezpečnosti: stanovuje základný rámec na bezpečné nakladanie s aktívami, uplatniteľný vo všetkých pracovných prostrediach vrátane práce na diaľku.

10.1.2 P3 – Politika prijateľného používania: upravuje primerané používanie zariadení a systémov organizácie počas práce na diaľku.

10.1.3 P4 – Politika riadenia prístupu: zabezpečuje, aby prístupové oprávnenia pre vzdialený prístup dodržiavali zásadu minimálnych oprávnení a správne mechanizmy autentifikácie.

10.1.4 P6 – Politika riadenia rizík: definuje spôsob identifikácie, ošetrenia a monitorovania rizík práce na diaľku v rámci ISMS.

10.1.5 P12 – Politika správy aktív: vyžaduje inventarizáciu aktív a riadenie konfigurácie pre všetky zariadenia používané na diaľku.

10.1.6 P22 – Politika logovania a monitorovania: zabezpečuje, aby vzdialené relácie boli monitorované, auditované a uchovávané podľa požiadaviek súladu.

10.1.7 P14 – Politika uchovávania a likvidácie údajov: definuje pravidlá nakladania s údajmi relevantné pre prácu na diaľku vrátane vymeniteľných médií a vyradenia zariadení.

10.2 Tieto politiky spoločne zabezpečujú, aby bola práca na diaľku bezpečná, v súlade s požiadavkami a uplatniteľná vo všetkých funkciách a geografických oblastiach.

11. Referenčné normy a rámce

11.1 Táto politika je zosúladená s medzinárodne uznávanými rámcami v oblasti bezpečnosti, ochrany údajov a riadenia rizík IKT s cieľom zabezpečiť bezpečné, sledovateľné a súladné postupy práce na diaľku.

11.2 ISO/IEC 27001

11.2.1 Kapitola 6.1.3 – plánovanie ošetrenia rizík: táto politika prispieva k ošetreniu rizík spojených so vzdialeným prístupom a distribuovanými pracovnými prostrediami.

11.2.2 Kapitola 8.1 – prevádzkové plánovanie a riadenie: vyžaduje implementáciu kontrol pre systémy, ku ktorým sa pristupuje mimo priestorov organizácie.

11.2.3 Príloha A, kontrola 6.7 – práca na diaľku: táto politika v plnom rozsahu pokrýva požadované kontroly informačnej bezpečnosti pri práci personálu mimo priestorov organizácie vrátane fyzických bezpečnostných opatrení, logického prístupu, riadenia prístupov a monitorovania správania používateľov.

11.3 ISO/IEC 27002:2022 – Kontrola 6

11.3.1 Táto kontrola vyžaduje procesné a technické ochranné opatrenia pre prácu na diaľku. Zahŕňa požiadavky na bezpečnosť zariadení, metódy prístupu, nakladanie s údajmi, ochranné opatrenia prostredia a riadenie účasti tretích strán, pričom všetky sú uplatnené prostredníctvom tejto politiky.

11.4 NIST SP 800-53 Rev.5

11.4.1 AC-17 (vzdialený prístup): priamo podporené prostredníctvom kontrol VPN, MFA, logovania relácií a schvaľovania prístupu na základe rolí pre vzdialených používateľov.

11.4.2 AC-2 (správa účtov): riadi oprávnenosť prístupu, prideľovanie vzdialených oprávnení a deaktiváciu účtov.

11.4.3 SC-12 až SC-13 (kryptografická ochrana, zavedenie kryptografických kľúčov): implementované prostredníctvom povinného používania VPN a celodiskového šifrovania na vzdialených koncových bodoch.

11.4.4 MP-5 (ochrana pri preprave médií) a PE-18 (umiestnenie komponentov informačného systému): požiadavky na prácu na diaľku stanovujú ochranu pri prenose a fyzické bezpečnostné opatrenia v prostrediach mimo pracoviska.

11.4.5 AU-2, AU-6: logovanie a monitorovanie vzdialených relácií podporujú požiadavky na audit a riešenie incidentov.

11.5 Nariadenie EÚ GDPR (2016/679)

11.5.1 Článok 32 – bezpečnosť spracúvania: táto politika vynucuje bezpečnosť vzdialeného prístupu, šifrovanie a kontroly logovania potrebné na ochranu osobných údajov, ku ktorým sa pristupuje alebo ktoré sa spracúvajú na diaľku.

11.5.2 Článok 5(1)(f): zabezpečuje, aby boli osobné údaje sprístupnené mimo pracoviska chránené pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou.

11.5.3 Odôvodnenie 39: zdôrazňuje obmedzenie prístupu, integritu a dôvernosť, čo je osobitne relevantné pri prenose zariadení mimo zabezpečených priestorov.

11.6 Smernica EÚ NIS2 (2022/2555)

11.6.1 Článok 21(2)(a, b, d): vyžaduje, aby bol vzdialený prístup zabezpečený ako súčasť rámca riadenia rizík IKT organizácie. Táto politika plní požiadavku na bezpečnostné opatrenia pokrývajúce riadenie prístupu, bezpečnosť údajov a organizačné pravidlá pre vzdialené prostredia.

11.6.2 Článok 21(3): podporuje bezpečnostné povedomie a uplatňovanie politík medzi pracovníkmi vykonávajúcimi prácu mimo centrálnych priestorov.

11.7 Nariadenie EÚ DORA (2022/2554)

11.7.1 Článok 5 – rámec správy a riadenia a vnútornej kontroly: táto politika podporuje očakávania na kontrolu rizík IKT vo všetkých prevádzkových scenároch vrátane hybridných modelov a práce na diaľku.

11.7.2 Článok 8 – rámec riadenia rizík IKT: riziká vzdialeného prístupu sú identifikované, zmierňované a riadené prostredníctvom technických a organizačných opatrení uplatňovaných touto politikou.

11.7.3 Článok 9 – mechanizmy zdieľania informácií: chráni pred vzdialeným únikom informácií zdieľaných v sieťach digitálnej prevádzkovej odolnosti.

11.8 COBIT 2019

11.8.1 DSS01 – riadené prevádzkové činnosti: táto politika podporuje bezpečnú kontinuitu činností bez ohľadu na fyzické umiestnenie.

11.8.2 BAI06 – riadené IT zmeny a BAI09 – riadené aktíva: zabezpečujú, aby boli zariadenia používané na prácu na diaľku sledované, bezpečne konfigurované a spravované ako kritické aktíva.

11.8.3 APO13 – riadená bezpečnosť: podporuje definovaný rámec správy a riadenia bezpečnosti pre vzdialené prostredia.

11.8.4 MEA03 – monitorovanie, hodnotenie a posudzovanie súladu: stanovuje, že činnosti práce na diaľku musia byť zaznamenávané v logoch, preskúmavané a auditované.