					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P09					Název dokumentu: **Politika práce na dálku**							
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**

1. Účel

1.1 Tato politika stanoví závazné požadavky na bezpečný výkon práce na dálku, včetně používání systémů organizace, přístupu k datům a plnění pracovních povinností mimo prostory společnosti.

1.2 Zajišťuje důvěrnost, integritu a dostupnost informačních aktiv přístupných na dálku a stanoví opatření ke zmírnění rizik spojených s distribuovaným pracovním prostředím.

1.3 Tato politika naplňuje požadavky přílohy A normy ISO/IEC 27001:2022, opatření 6.7, zavedením technických a procesních ochranných opatření přizpůsobených podmínkám práce na dálku.

2. Rozsah

2.1 Tato politika se vztahuje na veškerý personál oprávněný vykonávat práci na dálku, včetně:

2.1.1 zaměstnanců (na plný úvazek, na částečný úvazek, smluvních pracovníků)

2.1.2 externích poskytovatelů služeb, konzultantů a dodavatelů

2.1.3 dočasných a projektových pracovníků se schváleným vzdáleným přístupem

2.2 Politika se vztahuje na:

2.2.1 přístup k systémům organizace prostřednictvím virtuální privátní sítě (VPN) nebo schválených nástrojů pro vzdálený přístup

2.2.2 nakládání s citlivými a regulovanými informacemi mimo zabezpečené prostory

2.2.3 používání zařízení ve vlastnictví organizace nebo soukromých zařízení (BYOD)

2.2.4 fyzická bezpečnostní opatření a logický přístup v prostředí práce na dálku

2.3 Tato politika se uplatňuje ve všech zeměpisných oblastech a časových pásmech, kde organizace práci na dálku umožňuje, a to v pravidelném, ad hoc i kontinuálním režimu.

3. Cíle

3.1 Zajistit, aby k interním systémům a informacím na dálku přistupovaly pouze oprávněné osoby.

3.2 Vynucovat šifrování, vícefaktorové ověřování (MFA) a ochranu koncových bodů ve všech způsobech vzdáleného přístupu.

3.3 Udržovat bezpečnostní stav odolný vůči hrozbám, jako jsou phishing, škodlivý kód, exfiltrace dat a neoprávněné vystavení systémů.

3.4 Stanovit pravidla pro přenos, ukládání a tisk citlivých dat v prostředí mimo pracoviště.

3.5 Zavést opatření fyzické bezpečnosti, která omezí viditelnost a neoprávněné pozorování během vzdálených relací.

3.6 Zajistit soulad s mezinárodními regulačními požadavky na vzdálený přístup k datům, včetně GDPR, směrnice NIS2 a nařízení DORA.

4. Role a odpovědnosti

4.1 Vrcholové vedení

4.1.1 Schvaluje tuto politiku a zajišťuje potřebné zdroje a její začlenění do činností HR, IT a bezpečnostního provozu.

4.1.2 Schvaluje kritéria způsobilosti pro práci na dálku a její uplatnění v jednotlivých organizačních útvarech.

4.2 Ředitel informační bezpečnosti (CISO) / manažer ISMS

4.2.1 Odpovídá za tuto politiku, její údržbu a její soulad s apetitem k riziku a regulačními požadavky.

4.2.2 Stanoví bezpečnostní opatření pro vzdálený přístup (např. šifrování, ochrana koncových bodů, časové limity relací).

4.2.3 Schvaluje ošetření výjimek a monitoruje účinnost kontrol.

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

9. Požadavky na přezkoumávání a aktualizaci

9.1 Frekvence přezkumu

9.1.1 Tato politika musí být přezkoumávána každoročně nebo častěji při:

9.1.1.1 zavedení nových technologií vzdáleného přístupu

9.1.1.2 významném rozšíření práce na dálku (např. iniciativy hybridního pracovního režimu)

9.1.1.3 vzniku nových hrozeb, zranitelností nebo incidentů spojených se vzdáleným prostředím

9.1.1.4 změnách relevantních právních nebo regulačních rámců

9.2 Vlastnictví a proces přezkumu

9.2.1 Vlastníkem politiky je ředitel informační bezpečnosti (CISO). Přezkum musí být koordinován s:

9.2.1.1 IT provozem a architekturou

9.2.1.2 HR a správou budov a majetku (z hlediska provozních dopadů a dopadů na pracovní prostory)

9.2.1.3 pověřencem pro ochranu osobních údajů (z hlediska soukromí a kontrol přeshraničních přenosů dat)

9.2.2 Aktualizace politiky musí být:

9.2.2.1 schváleny Řídicím výborem pro bezpečnost informací

9.2.2.2 oznámeny všem dotčeným zaměstnancům a smluvním pracovníkům

9.2.2.3 začleněny do materiálů pro onboarding a pravidelné opakovací školení

9.3 Řízení dokumentu a distribuce

9.3.1 Politika musí zahrnovat správu verzí, datum účinnosti a historii změn.

9.3.2 Nahrazené verze musí být uchovávány v souladu s Politikou správy dokumentů (P14).

9.3.3 Revidované verze musí vyvolat povinné opětovné potvrzení seznámení u uživatelů způsobilých pro práci na dálku.

10. Související politiky a vazby

10.1 Tato politika se uplatňuje ve spojení s následujícími dokumenty:

10.1.1 P1 – Politika informační bezpečnosti: Stanoví základní rámec pro bezpečné nakládání s aktivy, který se vztahuje na všechna pracovní prostředí včetně práce na dálku.

10.1.2 P3 – Zásady přípustného užívání: Upravují přiměřené používání zařízení a systémů organizace během práce na dálku.

10.1.3 P4 – Politika řízení přístupu: Zajišťuje, aby oprávnění pro vzdálený přístup odpovídala zásadě minimálních oprávnění a řádným mechanismům ověřování.

10.1.4 P6 – Politika řízení rizik: Stanoví, jak jsou rizika práce na dálku v rámci ISMS identifikována, ošetřována a monitorována.

10.1.5 P12 – Politika správy aktiv: Vyžaduje inventář aktiv a řízení konfigurace pro všechna zařízení používaná na dálku.

10.1.6 P22 – Politika protokolování a monitorování: Zajišťuje, aby vzdálené relace byly monitorovány, auditovány a uchovávány v souladu s požadavky na soulad.

10.1.7 P14 – Politika uchovávání údajů a likvidace: Stanoví pravidla nakládání s daty relevantní pro práci na dálku, včetně výměnných médií a likvidace zařízení.

10.2 Tyto politiky společně zajišťují, aby práce na dálku byla bezpečná, v souladu s požadavky a vymahatelná napříč všemi funkcemi a zeměpisnými oblastmi.

11. Referenční normy a rámce

11.1 Tato politika je v souladu s mezinárodně uznávanými rámci pro bezpečnost, ochranu údajů a řízení rizik v oblasti ICT, aby zajistila bezpečné, dohledatelné a souladné postupy práce na dálku.

11.2 ISO/IEC 27001

11.2.1 Článek 6.1.3 – plánování ošetření rizik: Tato politika přispívá k ošetření rizik spojených se vzdáleným přístupem a distribuovaným pracovním prostředím.

11.2.2 Článek 8.1 – provozní plánování a řízení: Vyžaduje zavedení opatření pro systémy, ke kterým je přistupováno mimo prostory organizace.

11.2.3 Příloha A, opatření 6.7 – práce na dálku: Tato politika plně pokrývá požadovaná opatření informační bezpečnosti pro situace, kdy personál pracuje mimo prostory organizace, včetně fyzických a logických opatření, správy přístupu a monitorování chování uživatelů.

11.3 ISO/IEC 27002:2022 – opatření 6

11.3.1 Toto opatření vyžaduje procesní a technická ochranná opatření pro práci na dálku. Zahrnuje požadavky na zabezpečení zařízení, metody přístupu, nakládání s daty, ochranná opatření pracovního prostředí a řízení zapojení třetích stran — to vše je vynucováno touto politikou.

11.4 NIST SP 800-53 Rev.5

11.4.1 AC-17 (vzdálený přístup): Je přímo podporován prostřednictvím kontrol VPN, MFA, protokolování relací a schvalování vzdáleného přístupu na základě rolí.

11.4.2 AC-2 (správa účtů): Řídí způsobilost k přístupu, přidělování vzdálených oprávnění a deaktivaci účtů.

11.4.3 SC-12 až SC-13 (kryptografická ochrana, zřizování kryptografických klíčů): Jsou implementována prostřednictvím povinného používání VPN a šifrování celého disku na vzdálených koncových bodech.

11.4.4 MP-5 (ochrana při přenosu médií) a PE-18 (umístění komponent informačního systému): Pokyny pro práci na dálku vyžadují ochranu při přenosu a fyzická ochranná opatření v prostředí mimo pracoviště.

11.4.5 AU-2, AU-6: Protokolování a monitorování vzdálených relací podporuje požadavky na audit a reakci na incidenty.

11.5 GDPR (2016/679)

11.5.1 Článek 32 – zabezpečení zpracování: Tato politika vynucuje opatření pro zabezpečení vzdáleného přístupu, šifrování a protokolování nezbytná k ochraně osobních údajů, ke kterým je na dálku přistupováno nebo které jsou na dálku zpracovávány.

11.5.2 Článek 5(1)(f): Zajišťuje, aby osobní údaje přístupné mimo pracoviště byly chráněny před neoprávněným nebo protiprávním zpracováním a náhodnou ztrátou.

11.5.3 Bod odůvodnění 39: Zdůrazňuje omezení přístupu, integritu a důvěrnost, zejména v situacích, kdy zařízení opouštějí zabezpečené prostory.

11.6 Směrnice NIS2 (2022/2555)

11.6.1 Článek 21(2)(a, b, d): Vyžaduje, aby byl vzdálený přístup zabezpečen jako součást rámce řízení rizik v oblasti ICT organizace. Tato politika naplňuje požadavek na bezpečnostní opatření pokrývající řízení přístupu, bezpečnost dat a organizační pravidla pro vzdálené prostředí.

11.6.2 Článek 21(3): Podporuje bezpečnostní povědomí a uplatňování politik mezi pracovníky vykonávajícími práci mimo centrální prostory.

11.7 Nařízení DORA (2022/2554)

11.7.1 Článek 5 – správa a řízení a rámec vnitřních kontrol: Tato politika podporuje očekávání v oblasti řízení rizik ICT pro všechny provozní scénáře včetně hybridních režimů a práce na dálku.

11.7.2 Článek 8 – rámec řízení rizik ICT: Rizika vzdáleného přístupu jsou zde identifikována, zmírňována a řízena prostřednictvím technických a organizačních opatření.

11.7.3 Článek 9 – mechanismy sdílení informací: Chrání před vzdáleným únikem informací sdílených v sítích digitální provozní odolnosti.

11.8 COBIT 2019

11.8.1 DSS01 – řízený provoz: Tato politika podporuje bezpečnou kontinuitu činností bez ohledu na fyzické umístění.

11.8.2 BAI06 – řízené změny IT a BAI09 – řízená aktiva: Zajišťují, aby zařízení pro práci na dálku byla sledována, bezpečně konfigurována a spravována jako kritická aktiva.

11.8.3 APO13 – řízená bezpečnost: Podporuje definovaný rámec správy a řízení bezpečnosti pro vzdálené prostředí.

11.8.4 MEA03 – monitorování, hodnocení a posuzování souladu: Stanoví, že činnost spojená s prací na dálku musí být protokolována, přezkoumávána a auditována.