| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sem vložte název registrované právnické osoby | | | | | | |
| Číslo dokumentu:<br>P09S | | | | | Název dokumentu:<br>**Politika práce na dálku** | | | | | | |
| Verze:<br>1.0 | | Datum účinnosti:<br>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 příslušnými normami a právními předpisy

| Norma/právní předpis | Kapitola/článek | Komentář |
|---|---|---|
| ISO/IEC 27001:2022 | Kapitola 6.1, 6.2, 8 | |
| ISO/IEC 27002:2022 | Opatření 6 | |
| NIST SP 800-53 Rev. 5 | AC-17, AC-2 | |
| Směrnice EU NIS2 | Články 21(2)(b), 21(2)(h) | NIS2 |
| Nařízení EU DORA | Článek 9 | DORA |
| COBIT 2019 | DSS05, APO13 | COBIT 2019 |
| GDPR EU | Článek 32 | GDPR |

**1. Účel**

1.1 Tato politika stanoví bezpečnostní požadavky pro zaměstnance a smluvní pracovníky vykonávající práci na dálku, včetně práce z domova, ze sdílených pracovních prostor nebo během cestování.

1.2 Jejím cílem je chránit důvěrnost, integritu a dostupnost informací společnosti, k nimž je přistupováno mimo prostředí kontrolované společností.

1.3 Tato politika zajišťuje soulad s mezinárodními normami a snižuje rizika, jako jsou neoprávněný přístup, ztráta dat a narušení služeb.

**2. Rozsah**

2.1 Tato politika se vztahuje na všechny pracovníky (zaměstnance, smluvní pracovníky, konzultanty a dočasné pracovníky), kteří při práci mimo pracoviště přistupují k systémům, sítím nebo datům společnosti.

**2.2 Zahrnuje:**

2.2.1 používání zařízení poskytnutých společností i soukromých zařízení

2.2.2 přístup prostřednictvím VPN, vzdálené plochy nebo cloudových služeb

2.2.3 bezpečné nakládání s informacemi mimo prostory společnosti

2.2.4 monitorování, řízení výjimek a vymáhání požadavků této politiky

2.3 Vztahuje se na plný i částečný režim práce na dálku, včetně ad hoc vzdáleného přístupu.

**3. Cíle**

3.1 Předcházet neoprávněnému přístupu k systémům společnosti nebo k citlivým datům během práce na dálku.

3.2 Zajistit, aby zařízení a komunikační spojení používaná mimo kancelář splňovala požadavky na výchozí konfigurace a minimální bezpečnostní standardy.

3.3 Udržovat kontrolu nad oprávněními vzdáleného přístupu a monitorováním.

3.4 Poskytovat zaměstnancům a vedoucím pracovníkům jasné pokyny pro bezpečné postupy práce na dálku.

3.5 Plnit požadavky ISO, NIS2, GDPR, DORA a COBIT vztahující se na vzdálenou a mobilní práci.

**4. Role a odpovědnosti**

**4.1 Generální ředitel**

4.1.1 Schvaluje režimy práce na dálku a monitoruje soulad.

4.1.2 Eskaluje bezpečnostní incidenty nebo opakovaný nesoulad.

4.1.3 Přezkoumává výjimky a zajišťuje návazná opatření po incidentech.

**4.2 IT podpora nebo externí poskytovatel IT služeb**

4.2.1 Zajišťuje bezpečný vzdálený přístup (např. VPN, MFA).

4.2.2 Uplatňuje zabezpečení koncových stanic, šifrování a konfiguraci zařízení.

4.2.3 Poskytuje uživatelům podporu a řeší technické bezpečnostní problémy.

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

**9. Požadavky na přezkum a aktualizaci**

**9.1 Každoroční přezkum politiky**

9.1.1 Generální ředitel a IT podpora musí tuto politiku každoročně přezkoumávat, aby odpovídala technologickým, personálním a právním změnám.

**9.2 Spouštěče dřívější aktualizace**

**9.2.1 Okamžitý přezkum je vyžadován po:**

9.2.1.1 závažném bezpečnostním incidentu souvisejícím s prací na dálku

9.2.1.2 změnách požadavků NIS2, GDPR nebo DORA

9.2.1.3 přechodu na novou technologii vzdáleného přístupu (např. jinou platformu VPN)

**9.3 Řízení verzí a archivace**

**9.3.1 Všechny verze politiky musí být:**

9.3.1.1 opatřeny datem a schváleny generálním ředitelem

9.3.1.2 označeny číslem verze

9.3.1.3 archivovány po dobu nejméně tří let

**9.4 Informování pracovníků**

9.4.1 Aktualizace politiky musí být oznámeny všem uživatelům pracujícím na dálku. U jakékoli významné změny je vyžadováno potvrzení seznámení.

**10. Související politiky a vazby**

**10.1 Tato politika navazuje na následující dokumenty a podporuje je:**

10.1.1 P2S – Politika rolí a odpovědností v oblasti správy a řízení: stanoví, kdo schvaluje vzdálený přístup a vykonává nad ním dohled

10.1.2 P4S – Politika řízení přístupu: stanoví bezpečné zřizování vzdáleného přístupu a postupy jeho odebrání

10.1.3 P6S – Politika řízení rizik: sleduje a vyhodnocuje rizika související s přístupem mimo pracoviště

10.1.4 P8S – Politika povědomí o informační bezpečnosti a školení: školí uživatele o rizicích práce na dálku a osvědčených postupech

10.1.5 P30S – Politika reakce na incidenty: upravuje reakci na incidenty vzdáleného přístupu, jako jsou úniky přihlašovacích údajů nebo ztráta zařízení

**11. Referenční normy a rámce**

**11.1 ISO/IEC 27001**

11.1.1 Kapitola 6.1 – plánování založené na rizicích pro scénáře vzdáleného přístupu

11.1.2 Kapitola 6.2 – řeší odpovědnosti HR v kontextu mobilní a vzdálené práce

11.1.3 Kapitola 8.1 – operativní plánování a řízení vzdálených procesů

**11.2 ISO/IEC 27002**

11.2.1 Opatření 6.7 – poskytuje praktické pokyny k zabezpečení vzdálené a mobilní práce

**11.3 NIST SP 800-53 Rev. 5**

11.3.1 AC-17 – řízení vzdáleného přístupu, ochrana relací a bezpečnostní monitorování

11.3.2 AC-2 – řízení účtů pro uživatele mimo pracoviště

**11.4 GDPR**

11.4.1 Článek 32 – vyžaduje ochranu osobních údajů již od návrhu a ve výchozím nastavení, včetně režimu práce na dálku

**11.5 Směrnice NIS2**

11.5.1 Článek 21(2)(b) – vyžaduje bezpečné používání sítí a informačních systémů

11.5.2 Článek 21(2)(h) – vyžaduje bezpečnostní opatření související s HR, včetně kontrol mimo pracoviště

**11.6 Nařízení DORA**

11.6.1 Článek 9 – vyžaduje, aby finanční subjekty udržovaly odolnost ICT ve všech provozních režimech, včetně vzdáleného přístupu

**11.7 COBIT 2019**

11.7.1 DSS05 – správa bezpečnostních služeb: zahrnuje ochranu koncových stanic a bezpečné postupy práce na dálku

11.7.2 APO13 – řízená bezpečnost: zajišťuje bezpečné zřizování a dohled nad riziky mobilního a vzdáleného přístupu