scaut

Standardy

Splňují vaše náborové procesy dnešní standardy?

S nárůstem geopolitického napětí a s rostoucím ohrožením strategických zdrojů, kritické infrastruktury a národní bezpečnosti je mnoho organizací ze zákona povinno plnit předepsané bezpečnostní požadavky.

Patříte do jedné z kategorií?

- **Energetika**
  Elektřina, ropa, plyn a vodík.
- **Logistika**
- **Bankovnictví a finanční trhy**
- **Zdravotnictví**
- **Pitná a odpadní voda**
- **Digitální infrastruktura**
- **Digitální služby**
  Vyhledávače, online obchody a sociální sítě.
- **Vesmír**
- **Poštovní a kurýrní služby**
- **Odpadové hospodářství**
- **Chemický průmysl**
- **Potravinářství**
  Včetně výroby, zpracování a distribuce.
- **Výrobní průmysl**
  Zdravotnické, počítačové a dopravní příslušenství.
- **Obranný a zbrojní průmysl**

Zabezpečení dodavatelského řetězce

Důkladné ověřování externích a “remote” pracovníků má zásadní význam pro zajištění souladu s předpisy.

Remote pracovníci a kontraktoři mají často k dispozici rozsáhlý přístup k fyzickým a digitálním zdrojům, které mohou být ohroženy, pokud jsou spravovány nedůvěryhodnými osobami.

Dodržování předpisů bude v budoucnu náročnější, protože vlády budou řešit rostoucí globální napětí a vaši zaměstnanci budou muset být dostatečně ověřeni.

Standardy: 2025 a další

Standardy a směrnice	Co se od vás očekává?
NIS2 Směrnice NIS2, která vstoupila v platnost 16. ledna 2023, navazuje na směrnici EU o kybernetické bezpečnosti NIS. Členské státy měly čas do 17. října 2024, aby směrnici převedly do svých vnitrostátních právních předpisů. To znamená, že dotčené organizace musí ze zákona plnit její požadavky od 4. čtvrtletí roku 2024.	• Pravidelně provádět bezpečnostní kontroly, aby se ověřila odbornost, spolehlivost a bezúhonnost zaměstnanců pracujících s citlivými informacemi a technologiemi. • Stanovení opatření pro řízení rizik. • Zavedení mechanismů pro řízení incidentů kybernetické bezpečnosti. • Řešení rizik kybernetické bezpečnosti v dodavatelském řetězci (včetně poskytovatelů služeb třetích stran). • Dodržování vnitrostátních předpisů v oblasti dohledu a reportingu.
CER Směrnice o **odolnosti kritických subjektů** ukládá členským státům EU povinnost přijmout zvláštní opatření, která zajistí, aby základní služby pro zachování kritických veřejných služeb nebo hospodářských činností byly na vnitřním trhu poskytovány bez narušení.	• Zavést proces kontroly zaměstnanců, ověřit odbornost, spolehlivost a bezúhonnost osob, které mají přístup ke kritické infrastruktuře. Minimem je ověření totožnosti a beztrestnosti. • Vytvořit a udržovat vlastní systém řízení rizik. • Zavedení postupů pro hlášení incidentů a krizové řízení. • Pravidelně testovat a kontrolovat účinnost bezpečnostních opatření a strategií odolnosti.
SOC 2 SOC 2 je dobrovolný standard pro organizace poskytující služby, který vypracoval Americký institut autorizovaných znalců (AICPA) a který určuje, jak by organizace měly spravovat údaje o zákaznících.	• Zavedení procesů ověřování zaměstnanců, které zajistí odbornost, spolehlivost a bezúhonnost osob pracujících s citlivými údaji. • Vytvářet a udržovat pravidla a postupy, kterými se řídí provoz služeb. • Provádět hodnocení rizik za účelem identifikace potenciálních hrozeb. • Pravidelné monitorování a audit účinnosti kontrolních mechanismů • Zajistit, aby byly komunikovány informace týkající se kontrol.
ISO 27001 ISO 27001 je mezinárodní norma pro systémy řízení bezpečnosti informací (ISMS). Poskytuje rámec pro vytvoření, zavedení, udržování a neustálé zlepšování systému řízení bezpečnosti informací v organizaci. Jejím cílem je chránit citlivé informace před hrozbami, jako jsou hackeři a malware, prostřednictvím zásad, procesů a kontrolních mechanismů.	• Podle bodu 6.1 musí společnosti zavést proces kontroly, který ověří všechny zaměstnance na plný, nebo částečný úvazek, dočasné pracovníky a dodavatele, aby se zajistilo, že přístup k informacím bude mít pouze způsobilý a vhodně vybraný personál. • Zavést systém řízení bezpečnosti informací (ISMS) odpovídající rizikům. • Provádět komplexní hodnocení rizik a zavádět kontrolní mechanismy ke zmírnění těchto rizik. • Uplatňovat cyklus plánuj-proveď-prověř-jednejj (PDCA) k zajištění neustálého zlepšování ISMS. • Vzdělávat zaměstnance o jejich rolích v systému ISMS.
ISO 37001 Je mezinárodní standard, který umožňuje organizacím všech typů předcházet, odhalovat a řešit korupci přijetím řady opatření, včetně zásad proti korupčnímu jednání zaměstnanců, dohledu nad dodržováním předpisů proti korupci, školení, hodnocení rizik a dalších.	• Zavedení postupů “Poznej svého zaměstnance“ (KYE) k zajištění důkladného ověření zaměstnanců, posílení personální bezpečnosti a ochrany před korupčními riziky. • Vypracovat a zavést protikorupční směrnice. • Provádění hloubkové kontroly za účelem identifikace a zmírnění rizik korupce. • Zavedení a sledování finančních a organizačních kontrol, které zabraňují korupci. • Zajistit školení na podporu kultury integrity a dodržování předpisů.